Cybersécurité et PME

David Tortel, Sylvain Forthomme

▶ **To cite this version:**

David Tortel, Sylvain Forthomme. Cybersécurité et PME. Sciences de l'ingénieur [physics]. 2014. hal-01781568

HAL Id: hal-01781568

https://minesparis-psl.hal.science/hal-01781568

Submitted on 30 Apr 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Cybersécurité et PME
Mémoire Corps des Mines

David Tortel, Sylvain Forthomme

28 septembre 2014

Ce document s'inscrit dans le cursus de formation des Ingénieurs des Mines. Il propose une étude approfondie sur les enjeux liés à la cybersécurité dans le microcosme des PME et tente de proposer des leviers aussi bien institutionnels qu'économiques qui favoriseraient la prise en compte de ces enjeux par les agents économiques concernés.

Ce document est la propriété de ses auteurs ; il est émis à titre personnel et ne saurait en aucun cas refléter une position officielle du Corps des Mines.

Résumé

Avec un préjudice financier mondial estimé autour de 445 milliards de dollars, le risque cyber ne peut plus être sous-estimé ni ignoré. Que ce soit pour leur propriété intellectuelle, en tant que points d'entrée privilégiés dans les systèmes d'information des grandes entreprises pour lesquelles elles soustraitent une partie de l'activité, ou tout simplement pour l'exploitation des ressources physiques de leurs systèmes, la catégorie des petites et moyennes entreprises est celle dont le nombre de victimes de cyber attaques augmente le plus rapidement pour atteindre aujourd'hui des chiffres vertigineux.

Cette étude tente de jeter les fondations d'une réponse possible à cette question afin à la fois de sauvegarder l'industrie française et son innovation, et de protéger la croissance des futurs champions industriels.

Comme réponse à cette problématique, ce rapport propose dans un premier temps une réflexion illustrée des méthodes d'infection les plus répandues en relation avec les motivations des groupes qui les orchestrent. Un guide d'hygiène comportementale élémentaire qui permet, à coût nul, de renforcer au travers d'un comportement plus averti, la sécurité de son système d'information est alors proposé pour réduire sa surface de risques.

Deux leviers économiques sont ensuite définis afin de favoriser l'émergence d'une politique incitative, plutôt qu'autoritaire, en matière de cybersécurité ; ces leviers devront être implémentés par la Banque de France dans son rôle d'évaluateur externe de crédit et par les compagnies d'assurance et permettront aux entreprises de trouver leur optimum économique entre l'application de mesures de sécurité et l'acceptation du risque résiduel.

Le paradigme technologique aujourd'hui prédominant qui repose sur une rente technologique sera également remis en question à la faveur d'un modèle *open source* qui favorise l'innovation et le développement d'une offre de qualité basée sur le service ; ce modèle est censé produire un terreau industriel fertile, les barrières à l'entrée afférentes étant bien moins importantes.

La notion de confiance sera alors posée et trouvera une réponse dans le développement d'un cadre de certification rigoureux qui portera à la fois sur les solutions et sur les prestataires ; ce cadre devra être élaboré par l'Agence Nationale de Sécurité des Systèmes d'Information.

Le rôle de l'Etat et des collectivités territoriales, dont une grande partie des admnisatrations possède une structure et une sensibilité à la cybersécurité équivalentes à celles des PME, sera également soulevé. Des solutions seront proposées de nature à favoriser l'émergence d'une offre dédiée à ces structures en matière de cybersécurité, tout en renforçant massivement leur niveau de sécurité aujourd'hui trop faible.

Enfin, la question de l'éducation et de la création de parcours qualifiants sera soulevée afin que l'Etat tire profit de l'excellence de ses profils scientifiques afin de former des experts qui contribueront à la création d'une offre souveraine reconnue sur la scène internationale.

Table des matières

1 Quelle légitimité pour le sujet **9**
- 1.1 La place des PME dans l'économie française . . . 9
- 1.2 La faible sensibilité des PME aux enjeux de cybersécurité . . . 11
- 1.3 L'exploitation d'une nouvelle niche d'activités criminelles . . . 12
  - 1.3.1 Une adaptation des criminels aux nouvelles technologies . 12
  - 1.3.2 Le besoin d'immédiateté des utilisateurs . . . 12
  - 1.3.3 Les impasses juridiques . . . 13
  - 1.3.4 La difficulté de la coopération internationale . . . 13
  - 1.3.5 Absence d'un pôle juridirectionnel spécialisé . . . 13
- 1.4 Les PME, une cible naturellement privilégiée . . . 14
  - 1.4.1 L'adaptation contrainte des grands groupes . . . 14
  - 1.4.2 Les PME, porte d'entrée vers les grands groupes . . . 14
  - 1.4.3 Peu sécurisées, les PME sont des cibles faciles . . . 14
  - 1.4.4 Source d'innovation, les PME sont ciblées lors de campagnes d'espionnage . . . 15
- 1.5 De la difficulté d'obtenir des chiffres fiables . . . 15

2 Taxonomie des motivations **18**
- 2.1 De la gratification personnelle à la recherche de profits . . . 18
- 2.2 L'Espionnage . . . 19
- 2.3 L'altération des systèmes . . . 20
  - 2.3.1 Le sabotage . . . 20
  - 2.3.2 L'altération des données . . . 20
  - 2.3.3 La prise en otage du système . . . 21
  - 2.3.4 Le défacement . . . 21
- 2.4 Utilisation des ressources de la victime . . . 22
  - 2.4.1 L'exemple du Russian Business Network . . . 22
  - 2.4.2 La valeur d'un système . . . 23

3 Une menace protéiforme **25**
- 3.1 Attaques ciblées vs attaques non ciblées . . . 25
  - 3.1.1 Un exemple de l'attaque de masse : le spam . . . 25
  - 3.1.2 Un exemple de l'attaque ciblée : le Spear Phishing . . . 28
- 3.2 Les modes de pénétrations et les règles d'hygiène associées . . . 29
  - 3.2.1 Modèle formel d'une attaque . . . 29
  - 3.2.2 Le Drive by download . . . 31
  - 3.2.3 Client side exploit . . . 36
  - 3.2.4 Les clés USB . . . 37
  - 3.2.5 Utilisation de macro . . . 41
  - 3.2.6 Direct download (fake av, plugin, addon) . . . 42
  - 3.2.7 Les réseaux pair-à-pair –P2P . . . 44

4 Les conséquences d'une infiltration **46**
- 4.1 Assurer un revenu . . . 46
  - 4.1.1 Ransomware . . . 46
  - 4.1.2 Extorsion . . . 47
  - 4.1.3 Click Fraud . . . 47
  - 4.1.4 La porte dérobée . . . 48

4.2 Espionnage 48
4.2.1 Keylogger 48
4.2.2 Spyware 48
4.3 Sabotage 49
4.4 Utilisation de ressources et conséquences associées 49
4.4.1 Utilisation du serveur de messagerie de l'entreprise 49
4.4.2 Utilisation des systèmes de l'entreprise, l'attaque DDOS . 50
4.4.3 Utilisation des ressources de l'entreprise pour la distribution de contenu illicite 50

5 Il n'existe pas de solutions évidentes 52
5.1 Antivirus - firewall 52
5.1.1 Le paradoxde de l'antivirus 52
5.1.2 La difficulté d'appréciation 52
5.1.3 Cas d'un Wifi public 53
5.1.4 Démarrage sur un système alternatif 54
5.1.5 Fonctionnement et limites de la détection par signature . 54
5.1.6 Fonctionnement et limites de la détection comportementale 55
5.1.7 Vulnérabilté dans l'AV 56
5.1.8 L'utilisation de l'antivirus reste un MUST 56
5.2 Le cloud computing 57
5.2.1 Définition du cloud computing 57
5.2.2 La délocalisation des données 57
5.2.3 La relation de confiance 57
5.2.4 Une confiance dans la certification ANSSI 58
5.2.5 La sécurité des utilisateurs finals 58
5.2.6 La sécurité des applications web 58

6 La cotation Banque de France 61
6.1 Le principe de la création monétaire 61
6.1.1 Création monétaire par la banque commerciale 61
6.1.2 La création monétaire par la banque centrale 61
6.2 Le principe de la cotation 61
6.2.1 La nécessité d'une cotation indépendante 61
6.2.2 Les organismes de cotation 62
6.3 La cotation Banque de France 62
6.3.1 Un rôle pédagogique 62
6.3.2 La diversité des risques appréciés 62
6.3.3 Intégration du risque cyber dans la cotation 63
6.4 Mise en pratique 63
6.4.1 Création d'un kit d'autoévaluation 63
6.4.2 Pousuivre le rôle pédagogique 64

7 Renforcement des mécanismes assurantiels 65
7.1 Business model d'une assurance 65
7.1.1 L'autoassurance 65
7.1.2 Le transfert vers un tiers 65
7.2 Le développement massif du secteur de la cyber-assurance 67
7.2.1 Un marché essentiellement etats-unien 67
7.2.2 La responsabilité des données 68

7.2.3 Les réglementations catalysent le développement du marché de l'assurance . . . 68
7.3 Mise en place d'une offre dédiée . . . 69
7.3.1 Un modèle existant pour les grands groupes . . . 69
7.3.2 Un embryon de modèle pour les PME . . . 69
7.3.3 Un modèle qui se cherche . . . 70
7.3.4 Constitution d'un cercle vertueux . . . 71

8 Développement d'un modèle basé sur une offre de service 72
8.1 Les efforts de l'Etat pour soutenir l'industrie . . . 72
8.1.1 A court terme, les pôles de compétitivité . . . 72
8.1.2 A moyen terme, les Programmes d'Investissement d'Avenir 73
8.1.3 A long terme, les plans pour la nouvelle France industrielle 73
8.2 Le modèle open source . . . 73
8.2.1 L'open source, à la base du fonctionnement d'internet . . 73
8.2.2 L'open source est un modèle de développement, pas un modèle économique . . . 74
8.2.3 Les sources de revenus . . . 74
8.2.4 Les sources de coûts . . . 75
8.3 La création d'un terreau industriel fertile . . . 75
8.4 La difficulté d'appréhension du logiciel libre dans le domaine de la sécurité . . . 76
8.5 L'auditabilité du code . . . 77
8.6 Le contrôle de la solution . . . 77
8.7 Ne pas perdre le contrôle de son SI . . . 77
8.8 La nécessité de la confiance . . . 78

9 Le renforcement de la demande au travers de la commande publique 79
9.1 Les collectivités territoriales présentent une structure similaire à celle des PME . . . 79
9.1.1 Illustration par le cas des établissements de santé . . . 80
9.1.2 Une sensibilité équivalente aux enjeux de cybersécurité . . 81
9.2 Intégrer la cyber sécurité au sein de l'Etat . . . 81
9.2.1 Intégrer la cyber sécurité dès la conception des nouveaux projets . . . 81
9.2.2 Sécurisation des systèmes étatiques . . . 82

10 L'Etat doit poursuivre son entreprise de sensibilisation et renforcer les dispositifs de formation 84
10.1 Une offre de sensibilisation ramifiée . . . 84
10.1.1 L'ANSSI . . . 84
10.1.2 La D2IE . . . 85
10.1.3 La DGCIS . . . 85
10.1.4 DGGN, DGSI, DPSD, ... 85
10.1.5 Une entité pour les gouverner toutes . . . 86
10.2 Contribuer à faire évoluer le rapport de l'individu à l'outil informatique . . . 86
10.2.1 Le rôle de l'éducation nationale . . . 86
10.2.2 Mise en place d'un parcours professionnel qualifiant . . . 87

Internet a considérablement modifié le rapport des entreprises au monde en mettant à leur disposition une formidable palette d'outils qui facilitent et accélèrent les processus de création de richesses. Internet permet l'établissement instantané de canaux de communication entre protagonistes indépendamment de leur position géographique, ainsi que la transmission, par ce canal, d'une information dématérialisée à une vitesse proche de celle de la lumière. C'est donc la notion d'instantanéité et le traitement automatisé de l'information jusqu'alors impossibles qui deviennent réalité, ouvrant la voie à de nouvelles perspectives et une plus grande réactivité.

Ces nouvelles possibilités ont révolutionné les modes de fonctionnement et ont complètement bousculé les organisations[122] en revisitant des raisonnements jusqu'alors établis. Peu à peu, tous les domaines se retrouvent réinventés et redessinés au travers du prisme des technologies de l'information et de la communication et des fonctionnalités qu'elles proposent, permettant ainsi l'emmergence de leviers de croissance autour des nouvelles pratiques de consommation. Le marché du ecommerce, illustration intéressante des nouveaux modes de consommation, s'élève par exemple en 2013 en France à plus de 51 milliards de dollars, en augmentation de plus de 13% en valeur sur un an[71].

Cependant cette hyperconnectivité engendre de fait une certaine exposition que tentent d'exploiter les activités criminelles qui se développent en marge de ces nouvelles technologies. En effet, bénéficiant des mêmes fonctionnalités, les cyber criminels tirent profit de l'anonymat que semble permettre internet afin de perpétrer des attaques automatisées à des coûts souvent réduits, depuis une localisation soumise à une législation souvent floue. Un système faiblement protégé peut ainsi aujourd'hui être compromis par un robot depuis n'importe quel point du globe, là où une proximité physique et une action humaine étaient jusque là nécessaires. Dans la mesure où la très grande majorité de l'information est désormais disponible sous forme numérique il est alors possible de récupérer cette information, voire de la modifier ou de la supprimer à l'insu de son propriétaire. C'est donc une toute nouvelle forme de criminalité qui est apparue avec l'avènement d'internet et qui poursuit sa croissance au fur et à mesure de l'évolution technologique.

Une illustration de cette dualité dans l'utilisation d'une fonctionnalité issue des nouvelles technologies peut être trouvée dans le cas particulier de l'email. Dans le monde c'est ainsi près de 196 milliards d'emails qui sont envoyés par jour[79], mais dont près de 70% sont en réalité des messages de type pourriels, néfastes la plupart du temps[80] , et très souvent envoyés afin de gagner un accès illégitime sur un système faiblement protégé.

Dans un contexte évolutif, la cybercriminalité augmente de manière considérable (les cyber attaques ciblées ont bondi de 91% en 2013)[137], et affectent particulièrement les petites et moyennes entreprises pour lesquelles le recours aux nouvelles technologie s'avère fondamental. Cette étude focalise en conséquence sur l'urgence de l'appropriation des enjeux de la cybersécurité au sein du microcosme des PME.

Il s'agit alors dans un premier temps, après avoir démontré la légitimité du sujet, de comprendre le mode de fonctionnement des attaques et des organisations criminelles qui les orchestrent afin de proposer un guide d'hygiène comportementale de la sécurité des systèmes d'information pour les PME.

Une fois établi ce guide de bonnes pratiques, il sera question d'apprécier les différents leviers économiques qui pourraient être mis en place en France afin de favoriser l'emmergence d'une politique incitative en matière de sécurité des systèmes d'information ; deux leviers principaux seront alors détaillés qui devront être implémentés par la Banque de France dans son rôle d'Evaluateur Externe de Crédit et par les compagnies d'assurance.

Le système actuel des solutions de sécurité qui repose sur une rente technologique sera ensuite questionné et un nouveau paradigme basé sur le logiciel libre sera proposé, comme un modèle générateur de valeur dans sa composition d'un écosystème orienté vers le service.

Enfin, le rôle de l'Etat sera questionné, d'une part dans son soutien à une offre industrielle souveraine au travers de l'intégration de la sécurité dans ses propres applications, et d'autre part dans la poursuite de son action de sensibilisation et de formation qui gagnerait à être coordonnée à un niveau interministériel.

Dans toute la suite on retiendra une définition de la cybersécurité légèrement dérivée de celle proposée par l'ANSSI. Dans ce cadre, la cybersécurité est un état recherché pour un système [numérique] lui permettant de résister à des événements [extérieurs] susceptibles de compromettre la disponibilité du système, son intégrité ou la confidentialité des données stockées, traitées ou transmises [1] et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité numérique et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense[47]

La cybersécurité cherche donc à défendre dans ce contexte tous les systèmes numériques, qu'ils soient connectés entre eux ou non ; cette catégorie de systèmes augmente d'ailleurs de manière colossale avec l'arrivé de l'internet des objets.

Si le premier réflexe, en matière de sécurité économique et de cybersécurité, pourrait consister à vouloir considérer le sujet au niveau européen, il apparaît que peu d'Etats de l'Union se sont dotés de moyens, d'outils, et d'organisation susceptibles d'apporter une réponse aux problématiques soulevées dans cette étude. Les Etats européens présentent ainsi une très grande disparité de maîtrise technique, et d'appréhension des enjeux relatifs à la cyberdéfense et à la cybercriminalité. Il est alors peu étonnant de constater que les capacités des relais européens spécialisés qui ont emmergé soient, à l'heure de la rédaction de cette étude, relativement limitées tant au plan opérationnel que financier [101].

1. le cas échéant

Ce constat d'un retard conséquent des instances européennes dans l'appropriation du sujet, associé au caractère souverain de la matière nous semblent de nature à légitimer l'action de l'Etat français sur les questions de cybersécurité, qu'il s'agisse du domaine de la défense ou de l'action au regard de ses implications économiques et judiciaires.

1 Quelle légitimité pour le sujet

Dans toute la suite, la notion de « petites et moyennes entreprises » (PME) sera entendue au sens de sa définition juridique proposée lors de la recommandation de la commision du 6 mai 2003 concernant la définiton des micros, petites et moyennes entreprise puis formulée à l'article 51 de la loi dite de Modernisation de l'Economie 2008 et plus précisément au décret n° 2008-1354 du 18 décembre 2008 relatif aux critères permettant de déterminer la catégorie d'appartenance d'une entreprise pour les besoins de l'analyse statistique et économique[90] . Concrètement, l'ensemble considéré regroupe les entreprises qui

- d'une part occupent moins de 250 salariés,
- d'autre part ont un chiffre d'affaire qui n'excède pas 50 millions d'euros,
- ou dont le total de bilan demeure inférieur à 43 millions d'euros.

1.1 La place des PME dans l'économie française

La contribution des PME dans l'économie française est essentielle à de nombreux égards.

Tout d'abord, les PME françaises regroupent 3,4 millions d'entités soit 99,9 % du tissu entrepreneurial français et 52 % de l'emploi salarié en France. Elles constituent sur ce dernier point la catégorie la plus dynamique en matière de création d'emplois depuis 2007. Elles participent enfin à la création nationale de valeur ajoutée à hauteur de 49 % [65] comme illustré par la figure 1.

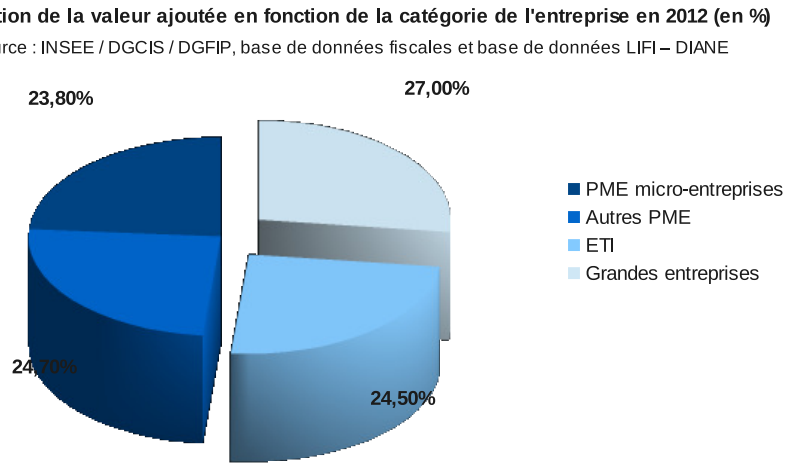

FIGURE 1 –

Leurs investissements en recherche et développement (R&D) en font la deuxième catégorie contributive sur le plan national. Ainsi en 2009, les PME de moins de 250 salariés représentaient 21% des dépenses intérieures de R&D en entreprise (à 5,63 Mds euros), alors que les dépenses des groupes de plus de 1000 salariés n'en représentaient que 62 % (à 16 Mds euros) comme illustré par la figure

2. Par ailleurs le montant total des dépenses émises par les PME en R&D a augmenté de 35% entre 2005 et 2009[?].

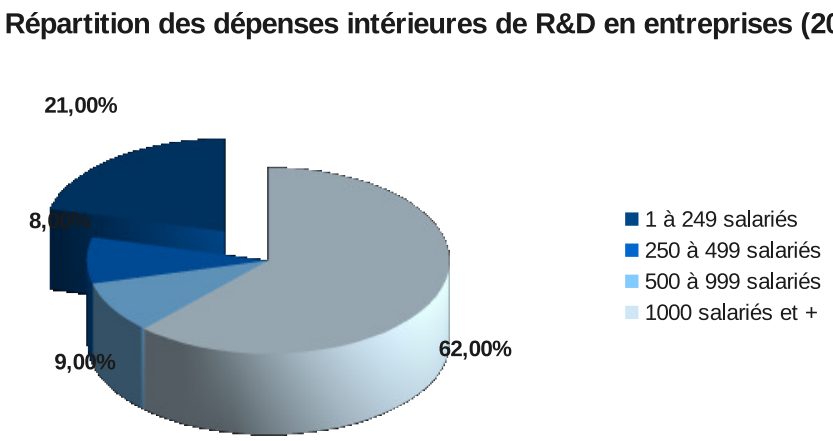

FIGURE 2 –

Enfin, les PME ont pleinement intégré la notion de propriété intellectuelle dans leur processus d'innovation. Malgré une production stable de brevets (autour de 2 %)[121], les PME adressent plus de la moitié des demandes de brevets délivrés parmi les personnes morales françaises ; le tableau 2 détaille la contribution respective des différents segments de la catégorie des PME.

TABLE 1 – Répartition du nombre de brevets en fonction du nombre de salariés

Salariés	Nombre de demandes publiées			Nombre de déposants			Nombre moyen de demandes par déposant	
	1999	2007	Variation	1999	2007	Variation	1999	2007
1 à 9	621	776	25%	529	621	17%	1,2	1,3
10 à 49	665	785	18%	523	535	2%	1,3	1,5
50 à 249	553	440	-20%	356	282	-21%	1,6	1,6
Total des PME	1839	2001	9%	1408	1438	2%	1,3	1,4

Lieux d'innovation, les petites et moyennes entreprises lancent et préfigurent les relais de croissance de demain, et sont de ce fait de potentielles cibles de croissance externes pour les grandes entreprises.

Il apparait par conséquent que le tissu économique français peut assez classiquement être distingué entre d'un côté les grandes entreprises, et à l'opposé, les petites et moyennes entreprises (PME). Les premières disposent avec certitude

de leviers humains et financiers leur permettant de s'adapter aux nouvelles exigences. A l'inverse, les secondes sont plus sujettes à subir le changement plutôt qu'à l'accompagner lorsqu'il s'avère étranger à leur coeur de métier.

1.2 La faible sensibilité des PME aux enjeux de cybersécurité

Le domaine particulier de la cybersécurité est illustratif de cette difficulté : là où les dirigeants de grandes entreprises peinent quant à l'identification des enjeux précis qui lui sont associés, les PME – sauf exception – n'ont qu'une très faible conscience des dangers afférents.

A titre d'exemple, une étude indépendante, menée par le *Ponemon Institute* en novembre 2013[128] sur l'ensemble du spectre des PME, s'attache à déterminer les principales raisons conduisant au manque de considération des risques induits par la cybercriminalité.

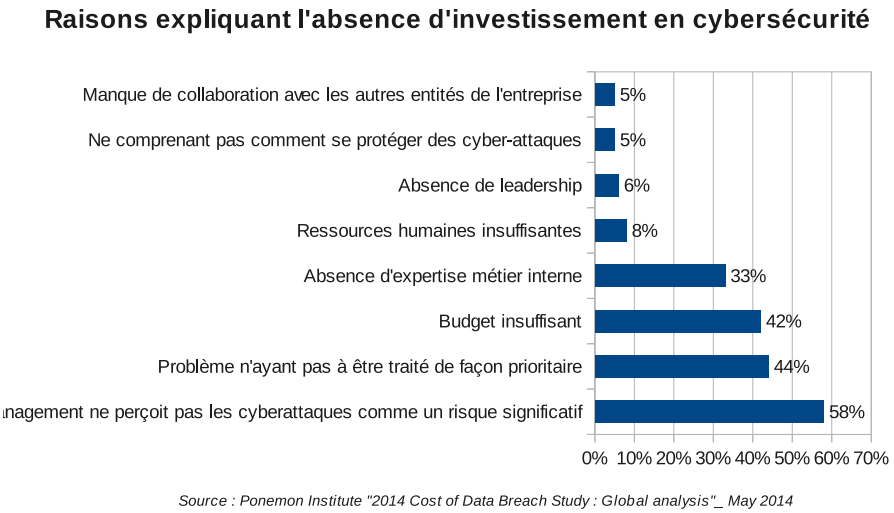

FIGURE 3 –

Les résultats, présentés par la figure 3, démontrent une situation plutôt inquiétante pour les PME, plus de la moitié d'entre elles n'identifiant pas les attaques cyber comme un réel significatif pour l'entreprise ou a minima comme l'une de leurs priorités.

Ce deuxième point s'explique certainement par le fait que les dirigeants des PME n'ont, dans la très grande majorité des cas, ni les moyens humains ou financiers à consacrer à la cybersécurité, ni les compétences suffisantes en interne pour aborder sereinement cette thématique. Par ailleurs, recruter un responsable de la sécurité du système d'information représente un coût non négligeable (environ 150 mille euros annuel[67]) que peu d'entre elles sont susceptibles de supporter.

Occupés à parfaire leurs offres de services ou de biens, et à maîtriser les délais et coûts de leurs fournisseurs, les chefs d'entreprises n'abordent finalement la sécurité de leur système d'information que de façon périphérique.

1.3 L'exploitation d'une nouvelle niche d'activités criminelles

1.3.1 Une adaptation des criminels aux nouvelles technologies

La cybercriminalité ne naît pas ex nihilo : il s'agit en fait bien souvent du prolongement des pratiques délictueuses et criminelles et de son adaptation à l'outil informatique et aux pratiques associées. Ainsi si le *quidam* se veut pleinement satisfait du nombre croissant des fonctionnalités offertes par l'outil numérique, ces évolutions induisent en réalité des fragilités qui sont rarement perçues, ou du moins ressenties comme telles.

Par exemple, là où auparavant l'usager devait se présenter au guichet de son agence bancaire pour requérir un virement, la dématerialisation des échanges lui offre aujourd'hui la possibilité d'ordonner un virement au moyen d'une simple connexion internet et depuis une quantité d'interfaces différentes (ordinateur, tablette ou téléphone portable,...). Cette facilité ergonomique procure une plus grande autonomie aux acteurs privés, mais elle crée également les conditions pour qu'un tiers, sous certaines conditions, puisse se substituer à ces derniers. L'industrie cybercriminelle a ainsi développé et diffusé des logiciels malveillants afin de répondre à cette nouvelle possibilité, le plus connu d'entre eux étant probablement le logiciel *Zeus*[134]

1.3.2 Le besoin d'immédiateté des utilisateurs

En outre, le regard porté par le citoyen sur l'outil informatique est assez étonnement naïf : par manque de connaissance technique, il accorde naturellement sa confiance aux échanges numériques et aux outils mis à sa disposition. Par ailleurs, le développement à grande vitesse de l'outil informatique, combiné à la rapidité d'accès et à l'immensité d'informations qu'offre internet, en des temps de l'ordre de la milliseconde, ont généré, dans l'inconscient collectif, un besoin d'immédiateté lorsqu'il s'agit d'accéder à une fonctionnalité. Dès lors, et quelles que soient les recommandations ou les risques en matière de sécurité, l'utilisateur moyen a tendance à adopter un comportement particulièrement irrationnel lorsque suivre une décision raisonné implique a une probabilité non nulle de subir un délai dans l'accès à la fonctionnalité requise.

L'illustration la plus simple de ce phénomène consiste à dénombrer le nombre de personnes utilisant les réseaux sans fil ouverts mis à disposition dans certaines grandes enseignes de restauration rapide ou dans de nombreux bars et cafés(voir 5.1.3, P53), ou encore de constater la proportion surprenante d'utilisateurs accéptant de poursuivre leur connexion vers une page web quand leur navigateur indique clairement que les informations renvoyées par le serveur ne sont pas conformes à ce qui est attendu et que la sécurité de la connexion est peut être compromise.

1.3.3 Les impasses juridiques

Bien entendu la criminalité traditionnelle a su identifier ces nouvelles potentialités, puis les exploiter en tirant par ailleurs avantage des insuffisances du cadre juridique : à supposer qu'il soit possible de retracer les attaques jusqu'à leurs auteurs (ce qui est déjà par essence particulièrement complexe[73]), comment ensuite appliquer un droit national alors qu'internet est une entité qui ignore par nature les frontières ? et quel droit lui appliquer ?

En France, la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, dite "loi Godfrain"[93] , permet de qualifier les infractions et délits relatifs à la criminalité informatique (ou plus exactement relative aux systèmes de traitement automatisé de données). Dans les faits, son efficacité s'avère limitée puisque réservée aux seuls faits commis sur le territoire français, mais sans permettre de poursuivre les personnes étrangères à l'origine de l'infraction.

Un second outil complète ce premier moyen, autorisant une coopération judiciaire lors de l'instruction entre les pays signataires : il s'agit de la convention de Budapest signée en 2001[61]. Néanmoins, cet accord ne couvre que les pays européens (qui l'ont de plus ratifié) et au-delà les pays avec lesquels des partenariats ont été développés ; il n'inclue nullement les pays en dehors de ce cadre, pays pourtant souvent à l'origine d'attaques comme la Chine, la Russie, les pays du Maghreb,...[141].

1.3.4 La difficulté de la coopération internationale

L'Union Européenne n'est pas en reste dans la lutte contre la cybercriminalité et la tentative d'approfondir la coopération entre les Etats de l'union ; elle a dans ce sens adjoint le Centre Européen de lutte contre la cybercriminalité (EC3) à Europol en janvier 2013. Cette entité mise en oeuvre dans le cadre de la stratégie de sécurité intérieure de l'UE adoptée en 2010, ne dispose toutefois que d'un budget très modeste de 7M euros en 2013[101], soit moins de 1/10ème de celui de l'ANSSI française[52]. Elle devrait cependant contribuer à centraliser l'expertise et l'information, et à soutenir les enquêtes criminelles à l'échelle de l'UE.

1.3.5 Absence d'un pôle juridirectionnel spécialisé

Enfin, un dernier constat s'impose en matière d'application du droit afférent sur le sol français : il n'existe aucun pôle juridictionnel spécialisé sur les questions de cybercriminalité. Cette absence engendre une relative hétérogénéité dans le traitement des procédures, ainsi qu'une difficulté à réprimer les atteintes graves aux systèmes d'information. Le sénateur Jean-Marie Bockel avait identifié et proposé de remédier à cette faiblesse[52] dans son rapport de décembre 2012 sur la Cyberdéfense, mais son appel n'a pour le moment guère été relayé.

Dès lors, le droit apparait comme un outils inadapté pour prévenir les délits organisés au travers de réseaux internationaux.

1.4 Les PME, une cible naturellement privilégiée

Face à l'évolution d'une criminalité inventive qui décide d'utiliser les possibilités nouvelles permises par la technologie, sans pour autant être fondamentalement inquiété par le droit existant, les PME ressortent comme des cibles idéales pour plusieurs raisons.

1.4.1 L'adaptation contrainte des grands groupes

Tout d'abord, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a prioritairement orienté son action vers la sensibilisation des grandes entreprises d'intérêt national délaissant de fait les PME non hautement stratégiques. En outre, l'exposition médiatique [2] accordée aux intrusions massives ayant visé des grands groupes comme AREVA[83], certaines révélations de Snowden[145], ou plus récemment l'ampleur des conséquences de certaines attaques outre mer [3] ont fortement aidé la prise de conscience des enjeux associés à la cybersécurité par cette catégorie d'acteurs économiques.

Leurs moyens conséquents au regard de ceux dévolus à une PME, leur ont par ailleurs permis de s'adapter à cette nouvelle donne. Ils ont alors su bénéficier de l'expertise et du savoir-faire, voire de solutions taillées sur mesure par les entreprises emblématiques du secteur de la défense comme Thales, Airbus Defense and Space ou encore Sogeti ...

La Loi de Programmation Militaire[91], loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale a de plus renforcé leurs obligations, instituant notamment pour chaque Opérateur d'Importance Vitale, dont la liste a été définie par l'ANSSI, le devoir de mettre en place des outils d'aide à la détection d'intrusion puis de reporter à l'autorité compétente toute attaque dont leur système d'information aurait fait l'objet[88].

1.4.2 Les PME, porte d'entrée vers les grands groupes

Face à cette évolution, les assaillants se sont adaptés en réorientant leurs actions vers des entreprises disposant d'un niveau de sécurisation inférieur. Cette réorientation se veut également très pragmatique : les PME, comme démontré précédemment s'avèrent peu sensibles aux enjeux de cybersécurité ; elles peuvent alors, par le biais de la sous-traitance intégrée, être utilisées comme un vecteur d'infection du SI de leur donneur d'ordre, mieux sécurisé[27].

1.4.3 Peu sécurisées, les PME sont des cibles faciles

Très nombreuses, les PME offrent par ailleurs la possibilité de multiplier les profits en passant une attaque à l'échelle : une fois connues les failles de certains logiciels largement répandus, les organisations criminelles peuvent décliner leur attaque auprès de toutes les sociétés vulnérables pour un cout marginal quasiment nul.

2. et relayée par les syndicats comme le medef

3. Target, le troisième groupe de la grande distribution américaine a été victime d'une attaque informatique dont le cout s'élève à 148 millions de dollars[43]

De plus, le niveau de sécurisation du SI d'une PME se limite dans la plupart des cas à celui du simple particulier, à savoir l'utilisation d'outils grand public comme un firewall ou un antivirus (voir 5 P52) alors que leur surface financière, supérieure à celles des personnes physiques, en font une cible plus favorable.

1.4.4 Source d'innovation, les PME sont ciblées lors de campagnes d'espionnage

Le fait d'être une source d'innovation importante peut également présenter un attrait pour d'autres acteurs économiques peu scrupuleux : certaines techniques de fabrication, le contenu de brevets, la propriété intellectuelle en somme, peuvent ainsi être dérobés à des fin d'appropriation dans le cadre de campagnes d'espionnage. Or, comme vu précédemment (voir 1 P9), les PME jouent un rôle particulièrement important dans la recherche et développement et dans le dépot de brevets, faisant d'elles des cibles intéressantes et de choix.

1.5 De la difficulté d'obtenir des chiffres fiables

Toutefois, la réalité des attaques "cyber" menées à l'encontre des entreprises françaises demeure impossible à déterminer en nombre et en valeur du préjudice encouru. Certains acteurs majeurs de la cybersécurité sont prompts à souligner une situation calamiteuse[116], que l'on peine à retrouver au sein des statistiques établies par la Direction Générale de la Gendarmerie Nationale[81] :

TABLE 2 – Nombres et variations annuelles des escroqueries et infractions assimilées commises par le biais d'Internet et enregistrés par la police et la gendarmerie entre 2009 et 2012

Infractions	2009	2010	2011	2012	Variation 2009 / 2012 (en volume et %)
Escroqueries et infractions économiques et financières commises sur Internet	37 357	33 928	33 944	29 796	
Variation en volume	-3 429	16 -4 148	-7 561		
Variation en pourcentage	-9%	0%	-12%	-20%	
Escroqueries et abus de confiance	28 044	27 225	27 259	27 928	
Variation en volume		-819	34	669	-116
Variation en pourcentage		-3%	0%	2%	0%
Falsifications et usages de cartes de crédit	9 313	6 703	6 685	1 868	
Variation en volume		-2 610	-18	-4 817	-7 445
Variation en pourcentage		-28%	0%	-72%	-80%

Entre les deux volumétries, le biais semble important, mais il existe à cela plusieurs raisons simples :

En dehors de la contrainte précédemment énoncée faite aux OIV depuis la Loi de Programmation Militaire, il n'existe aucune obligation légale pour une personne physique ou morale de porter plainte suite à une attaque "cyber" dont elle aurait été victime, ni même de la signaler (exception faite des fournisseurs d'accès dont la notification des violations de données à caractère personnel est rendue obligatoire par l'article 34 bis de la loi informatique et libertés[32]).

Révéler le préjudice peut par ailleurs, s'avérer contre-productif pour les raisons suivantes :

- cela nuit à l'image et à la réputation de l'entreprise, sans qu'elle puisse en attendre un retour direct.
- porter plainte signifie également que l'on est en règle avec les déclarations CNIL (Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende[87].) ; or ces contraintes administratives sont souvent négligemment oubliées par les PME[63]

Par ailleurs, et c'est peut être le point le plus caractéristique, révéler une attaque signifie d'abord et avant tout que l'on ait pris conscience de cette attaque, ce qui nécessite bien souvent des outils de détection et d'analyse dont ne disposent pas les PME..

Enfin, les statistiques les plus alarmantes proviennent de sociétés antivirus dont le coeur de métier reste de vendre des solutions afin de prévenir les dites attaques. Il n'est par conséquent pas à exclure que ces chiffres soient artificiellement revus à la hausse dans une entreprise marketing visant à jouer sur l'instauration d'un climat d'appréhension.

La réalité doit en conséquence se trouver quelque part entre les deux approches statistiques. Toutefois, et malgré les divergences, les acteurs s'accordent dans l'identification de deux tendances majeures :

- Les PME sont le groupe des victimes dont le nombre croît le plus rapidement[137] [127]
- La cybercriminalité oriente ses efforts sur les outils nomades (tablettes, téléphones portables) moins sécurisés.

Il apparait au terme de cette première partie d'analyse que si la catégorie des PME est en quelque sorte la colonne vertébrale de l'économie et de l'innovation en France, au travers respectivement de ses partenariats avec les grands groupes et de ses efforts prolongés pour la recherche et le développement, les dirigeants d'entreprise n'ont pas su prendre la mesure des risques induits par l'arrivée des nouvelles technologies, faisant de ce groupe une cible *facile* qu'il est urgent de considérer. Par ailleurs, les contraintes notamment budgétaires très fortes auxquelles doivent faire face les PME, combiné à l'extrême variété des besoins métiers imposent de trouver des solutions qui soient à la fois particulièrement modulables et dont les premiers niveaux soient dans des prix abordables.

Enfin, il est important de prendre conscience que les problèmes de cyber sécurité ne concernent pas uniquement les PME qui seraient ciblées par des attaques de type *Advanced Persistent Threat*[4], la plupart d'entre elles étant en réalité atteintes de façon aléatoire au gré de la propagation des infections[5]. Cette distinction est fondamentale dans la mesure où elle appelle des réponses différentes et justifie la question des modèles qui motivent les cyberattaques.

4. Une *Advanced Persistent Threat est une attaque ciblée et orchestrée de longue date par des réseaux de cybercriminels organisés et déterminés*

5. Lors de nos entretiens avec la DGSI il est apparu que la répartition (calculée de manière complètement empirique) des infections au sein des PME se découpait comme suit : 10% d'attaques ciblées, 90% d'infection par des attaques de masse non ciblées

2 Taxonomie des motivations

S'intéresser à la cybersécurité nécessite d'avoir une compréhension fine des causes qui se cachent derrière les cyberattaques et des organisations qui les orchestrent. Il apparaît effectivement indispensable d'avoir une bonne connaissances des protocoles opératoires utilisés et d'analyser de manière précise les motivations qui sous-tendent les cyber-attaques afin d'être en mesure de protéger les bonnes ressources et de connaître les points sensibles à scruter méticuleusement. Un bref coup d'oeil dans le rétroviseur suffit d'ailleurs à démontrer que les desseins des *"codeurs de virus"* se sont transformés avec le temps, passant d'une recherche de la reconnaissance à la volonté de création d'une arme de destruction ciblée.

Cette partie ainsi que les deux suivantes sont ponctuées de règles et recommandations qui ont pour objectif de respectivement combattre certaines idées reçues et offrir un cadre de règles d'hygiène comportementale élémentaire. Il s'agit d'un guide pratique énumérant des points fondamentaux à retenir et à appliquer afin d'améliorer significativement, à coût nul, le niveau de sécurité des PME.

2.1 De la gratification personnelle à la recherche de profits

Le visage de la cybercriminalité a beaucoup évolué sur les dix dernières années. Les premiers programmes malveillants se propageaient à une vitesse impressionnante et avaient une charge active qui se voulait visible par l'utilisateur. La motivation s'orientait alors vers la recherche d'une couverture médiatique la plus importante possible et donc la recherche d'une gratification personnelle[138]. Il était dans ce contexte important que l'utilisateur puisse être témoin de l'activité néfaste du virus et s'en fasse ensuite le relais afin que le programme malveillant gagne une couverture médiatique forte.

Ces comportements très agressifs des premiers virus ont d'ailleurs à ce point conditionné les esprits des utilisateurs que beaucoup sont aujourd'hui persuadés que leur système n'est pas compromis dans la mesure où celui-ci ne donne pas de signe clair et évident de compromission (comme ce pouvait être le cas avec les premiers programmes malveillants). Soutenir ce propos revient à ignorer la profonde mutation des motivations des créateurs de virus qui tentent désormais de développer les programmes les plus discrets et les plus indétectables possibles afin de maintenir un accès sur le système aussi longtemps que faire se peut.

Règle 1 : Un système peut être compromis et ce même si aucun comportement suspect n'est détecté ni par l'utilisateur ni par un autre autre programme (type antivirus).

Les pratiques de développement de virus ont donc évolué depuis les dix dernières années pour donner naissance à l'émergence d'une activité cybercriminelle qui a trouvé un business modèle particulièrement rentable[140] et qui cherche désormais avant tout l'enrichissement de la structure au moyen de manoeuvres malhonnêtes. On assiste ici au développement de tout un écosystème

cybercriminel voyant dans l'informatique leur arme de choix, et dans la recherche de profit la principale motivation. Cette recherche de profit peut être projetée sur les trois axes détaillés ci-dessous, chacun regroupant en quelques sortes une famille de motivations : L'espionnage, Motivations relatives à l'altération des données, L'utilisation des ressources du système.

2.2 L'Espionnage

Le 29 Septembre 2011[83] le mensuel l'Expansion révèle ce qui restera comme un des événements qui a le plus marqué les dirigeants d'entreprises françaises en matière de cybersécurité. AREVA, leader mondial de l'énergie nucléaire a été infiltré, et l'attaque dure depuis plus de deux ans. Cette attaque a pour objectif d'exfiltrer les données sensibles dans le but de s'approprier les ressources et la propriété intellectuelle du groupe.

L'espionnage, motivation particulièrement bien relayée par les médias dans le cadre de cyber-attaques, est à présent étroitement lié dans l'inconscient collectif (voire de manière quasi surjective) aux motivations qui sous-tendent les incidents de sécurité. Par ailleurs, les révélations Snowden[145] ont largement contribué à l'amalgame, suggéré par la presse et diffusé par les relais d'opinion, entre attaques cyber et espionnage des grandes puissances (qu'elles soient commerciales ou militaires) ; l'outil informatique se fait dans ce contexte le fer de lance d'une politique d'intelligence économique poussée à son paroxysme.

Cependant, cette perception dévoyée par un prisme fantasmé et déformé tend à déresponsabiliser le simple utilisateur ou l'employé de la PME, celui-ci ne se sentant absolument pas concerné par tous ces enjeux qui le dépassent et vis-à-vis desquels il se sent de toute façon impuissant.

Or, comme vu précédemment, la PME peut également se retrouver au centre d'une campagne d'espionnage dans les cas suivants :

- La PME travaille sur un produit innovant
- La PME est le sous traitant d'un grand groupe

Le vol de propriété intellectuelle est estimé autour de 400 milliards de dollars[107] par an ; au premier rang des victimes, les PME dont on a déjà démontré qu'elles jouent un rôle majeur dans la recherche et l'innovation (voir 1, P9).

Par ailleurs, les méthodes d'intrusion ont également évolué ces dernières années, passant d'attaques directes à des attaques par rebonds. Il est alors le plus souvent bien moins difficile pour une entité criminelle désirant pénétrer le système d'information d'un grand groupe de passer par le sytème d'information d'un de ses sous-traitants, très probablement moins bien sécurisé, et d'utiliser ensuite son accès vers le système du groupe visé inititalement.

Règle 2 : Une PME, ou un particulier, peut se retrouver au centre d'une campagne d'espionnage, et ce même sans en être la cible principale. Elle devient alors le vecteur d'intrusion.

2.3 L'altération des systèmes

La seconde des motivations peut être trouvée dans la volonté d'altération des systèmes ; cette altération peut prendre plusieurs formes, jusqu'à la destruction des systèmes, en passant par la modification des données qu'ils contiennent.

2.3.1 Le sabotage

Le sabotage s'apparente à la destruction pure et simple de systèmes ou de données afin de tirer un avantage économique ou psychologique sur sa cible. Une fois pénétré le système d'information de sa victime, l'attaquant peut alors littéralement détruire les données qu'il contient.

Destruction des systèmes et des données Une telle attaque a par exemple eu lieu en août 2012 lorsque plus de 30 000 ordinateurs appartenant à la société Saudi Aramco ont été formatés[120], entrainant la perte sèche de toutes les données et engendrant un coût de reprise d'activité colossal. La réitération de ce schéma sur une entreprise française, en particulier un Organisme d'Importance Vitale, demeure d'ailleurs l'une des principales craintes de l'ANSSI[105].

Déterioration des outils ou produits Il est par ailleurs possible avec le développement massif de l'informatique industrielle de modifier le comportement des composants industriels physiques afin d'affaiblir la qualité de la production ou de détériorer le matériel industriel. L'exemple le plus classique de ce type d'attaque reste probablement le vers Stuxtnet[146] dont la charge malveillante reprogrammait les automates industriels Siemens afin d'accélérer la vitesse de rotation de centrifugeuses et d'appauvrir ainsi la qualité de l'uranium produit tout en dupant les sondes de contrôle dans le but de camoufler son activité et de dégrader physiquement les matériels.

Une fois de plus, si la PME peut ne pas être une cible directe pour ce genre d'attaques d'une grande complexité, elle peut cependant être un vecteur véhiculant la menace vers un groupe pour lequel elle travaille.

Règle 3 : Une PME, ou un particulier, peut se retrouver au centre d'une campagne de sabotage même sans en être la cible principale. Elle devient alors le vecteur d'intrusion.

2.3.2 L'altération des données

L'altération des données consiste à sciemment modifier des données métier afin de tirer profit de cette modification.

Lors des entretiens préalables à la rédaction de ce rapport, il est apparu une illustration de ce cas de figure ; une PME française bien reconnue dans son domaine de compétences et avec un carnet de commandes jusqu'alors bien rempli s'étonne de ne plus recevoir de nouveaux contrats. La raison ? Tous les emails envoyés par l'équipe commerciale étaient reroutés vers une société concurrente qui modifiait alors les propositions commerciales en majorant tous les tarifs de 30% avant de transférer l'email au destinataire légitime. Les différents clients,

s'étonnant du tarif des prestations se retournaient alors vers les sociétés concurrentes.

2.3.3 La prise en otage du système

La prise en otage des systèmes devient également une attaque de plus en plus répendue. Dans ce scénario, le système compromis est altéré de manière importante et les cybercriminels n'acceptent de le remettre en état qu'après remise d'une rançon.

2.3.4 Le défacement

Le défaçage, ou défacement consiste pour un attaquant à défigurer une page web à la suite d'un piratage. En 2005, en France, cela a constitué 3% des sinistres informatiques[68]. Les cibles sont multiples, en partant des journaux type The Sun, Synday Times ou encore Reuteurs[50] en passant par les hôpitaux, collectivités territoriales ou clubs de football[48]. Toutes les pages web peuvent ainsi en être victimes.

Si la motivation derrière un défacement peut être de plusieurs ordres, elle cherche d'abord à nuire à l'image de l'entreprise défacée et/ou à véhiculer un message partisan. C'est par exemple pour protester contre la fermeture du site *Megaupload* que les *Anonymous* ont rendu inaccessibles en les défaçant les site de *Vivendi*, *Universal* et *Warner*[78], comme l'illustre la Figure 4. Sur le site web de Vivendi, on pouvait alors lire ce message : *"Anonymous accuse Vivendi d'actes de censure et de haute trahison envers l'esprit d'Internet. Par sa participation au lobbying culturel, Vivendi se rend coupable de pression anti-démocratique auprès des gouvernements, et est directement responsable de l'acte de guerre intenté par le FBI contre la communauté d'Internet"*

Au delà du déficit d'image qu'elle engendre, une telle attaque peut ainsi mettre la société visée hors service, en ne permettant plus l'affichage des pages d'information ou de commandes.

La motivation peut également être plus directement économique. En défaçant le site, le cybercriminel ajoute alors virtuellement à chaque connexion sur la page web une action de l'utilisateur qui consiste à simuler un clic vers un lien sponsorisé. Or le modèle du paiement par clic, modèle publicitaire dans lequel un éditeur de contenu (un site web) est rémunéré par un annonceur proportionnellement au nombre de clics uniques vers les bannières publicitaires de ce dernier, étant un des modèles publicitaires les plus répandus, le cybercriminel se retrouve rémunéré à chaque connexion sur le site (voir 4.1.3, P47).

Le défacement peut donc servir plusieurs motivations, depuis un intérêt dans une guerre économique de moyenne à grande envergure vers un simple intérêt pécunier pour l'attaquant en passant par la volonté de trouver une nouvelle vitrine pour afficher un message partisan. Dans ce cas, le cybercriminel utilise les ressources du système d'information cible à son avantage ; il s'agit alors d'un corollaire de la dernière grande famille de motivations : l'utilisation des ressources de la cible.

FIGURE 4 – Exemple de défaçage du site web de Vivendi suite à la fermeture de *Megaupload*

2.4 Utilisation des ressources de la victime

Comme nous l'avons démontré, la plupart des attaques sont menées dans un objectif de profit, qu'il soit directement pécunier, ou qu'il serve des intérêts particuliers dans la guerre économique. La perspective de l'argent facile aidant, de nombreuses organisations se sont lancées dans ce type de business ; pour répondre au besoin naissant qui apparaissait, elles ont développé des offres diverses, depuis le développement de virus jusqu'à la location d'un parc de machines pour mener une attaque de Déni de Service (voir 4.4.3 , P50). Certaines de ces organisations proposent même un service après vente ou une garantie antivirus[54]. Le *malware Turkojan* par exemple propose dans sa version *premium* jusqu'à six mois de remplacement du produit s'il est détecté par un antivirus, ainsi qu'un support technique via email ou messagerie instantanée, tel qu'illustré par la figure 5.

2.4.1 L'exemple du Russian Business Network

Une des organisations de cybercriminels les plus réputées aujourd'hui reste probablement le *Russian Business Network* (RNB)[1] . Son étude permet de comprendre les enjeux qui se cachent derrière les attaques de grande ampleur. Cette organisation se concentre principalement sur 6 centres d'intérêt :

- Le phishing
- Le scam
- Le commerce de logiciels malveillants
- La location de machines zombies pour des opérations de Dénis de service
- La pornographie (incluant la pédopornographie)
- Les jeux d'argent

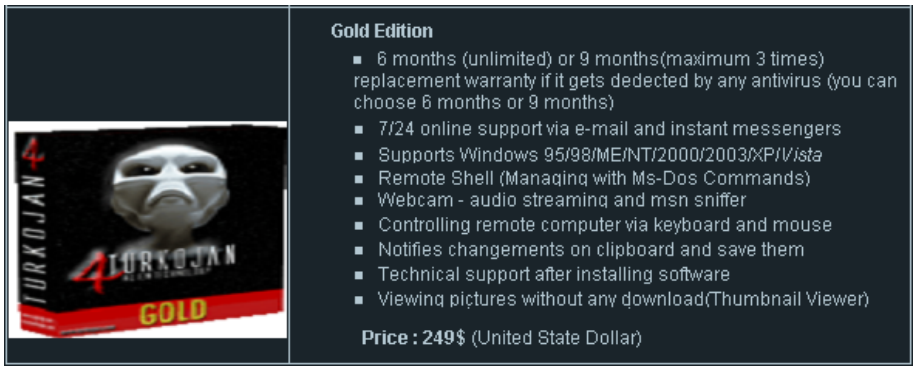

FIGURE 5 – Le marché des logiciels malveillants se développe en utilisant les codes du marketing et en proposant des services après vente

2.4.2 La valeur d'un système

Pour mener à bien ses opérations, l'organisation a besoin d'une quantité importante de ressources, que ce soit pour le développement de sa capacité de calcul, pour l'augmentation de sa bande passante ou tout simplement pour bénéficier d'une plateforme d'hébergement bon marché mais surtout qui puisse passer à l'échelle et qui soit résiliente afin que l'arrêt de parties du réseau (par les autorités) n'empêche pas le bon fonctionnement du reste de l'activité.

De nombreuses campagnes, attaques et virus sont donc lancés sur internet dans le seul but d'acquérir et de diversifier au maximum ses ressources.

Il apparaît ici clairement que l'on n'est pas forcément la cible d'une cyberattaque pour une donnée en rapport avec son activité, mais que la simple ressource que constitue le système peut justifier à elle seule une attaque. Le système devient alors une fois qu'il est compromis une partie de la plateforme d'hébergement de l'organisation criminelle et peut ainsi se retrouver complice d'une activité répréhensible par la loi, comme l'hébergement et la mise à disposition de contenus pédopornographiques, de sites de jeux ou d'arnaques[149] et ainsi se retrouver au coeur d'une procédure judiciaire.

Règle 4 : Un système relié à internet est forcément une cible pour une organisation malveillante : soit pour les données qu'il contient, soit pour la ressource qu'il constitue.

Les paragraphes précédents se concentrent sur des attaques semblant provenir la plupart du temps de l'extérieur de l'entreprise ; il est cependant particulièrement important de se rappeler que près de la moitié des attaques sont exécutées par des ex-salariés (ou avec leur aide) pour des motifs pécuniers ou liés à la vengeance personnelle. Par ailleurs dans la mesure où le turn over est aujourd'hui très important dans les sociétés, il est fondamental de protéger l'information (que ce soit l'information métier ou celle relative aux différents systèmes) même à l'intérieur de l'entreprise afin que le personnel ne puisse pas être en mesure de faire fuiter ces informations vers l'extérieur. De telles mesures

nécessitent donc une gestion des droits d'accès rigoureuse ; cet aspect n'est cependant pas traité dans cette étude qui focalise avant tout sur la sécurité des systèmes et non la sécurité de l'information.

Tous les systèmes connectés sont des cibles en devenir. La partie suivante tente de mettre en évidence les méthodes les plus souvent employées par les cybercriminels pour pénétrer les systèmes d'information.

3 Une menace protéiforme

Cette partie tente d'établir certaines règles pratiques d'hygiène comportementale élémentaire. Il n'est en aucun cas question ici de réécrire, de répéter ou de compléter le guide d'hygiène informatique proposé par l'ANSSI[46] à destination des DSI ou RSSI, mais plutôt de fournir une liste non exhaustive de conseils de base destinés à élever le niveau de vigilance des utilisateurs. Ces règles ont pour vocation d'être applicables par la plupart des particuliers et PME, et leur mise en oeuvre bien que ne coutant rien sur le plan financier peut améliorer de manière significative la sécurité des systèmes.

3.1 Attaques ciblées vs attaques non ciblées

Comme démontré dans la partie précédente, on peut catégoriser les attaques informatiques en 2 grandes familles :

- Les attaques ciblées [type espionnage, sabotage, defacement,...]
- Les attaques de masse [type défacement, utilisation des ressources,...]

Nous démontrons ici que la plupart des attaques de masse peuvent être évitées au moyen de mesures simples d'hygiène comportementale. Très souvent, le cas d'attaque de masse laissera en effet des traces comme des indices qui devront indiquer qu'une menace guette.

Règle 5 : Les attaques non ciblées peuvent souvent être évitées au moyen de mesures simples d'hygiène comportementale

3.1.1 Un exemple de l'attaque de masse : le spam

Le spam est un courrier électronique non sollicité. Il s'agit dans la plupart des cas de messages envoyés en masse. Ces messages peuvent être à visée publicitaire, ou, dans le cas d'une campagne d'attaque, à visée criminelle ; ils sont alors envoyés afin de gagner un accès sur la machine de la victime.

Prenons l'exemple d'un message de spam et voyons comment il est possible, au moyen de mesures simples de s'apercevoir qu'il s'agit effectivement bien d'un message illégitime :

A la réception de l'email, le destinataire doit se poser les questions suivantes :

- L'adresse de l'expéditeur est-elle en rapport avec l'entité d'envoi ?
- L'adresse du destinataire est-elle bien mon adresse ?
- Le message m'est-il personnellement destiné ?
- Le contenu de l'email comporte-t-il un nombre important de fautes d'orthographe ?
- Le contenu de l'email est-il une image contenant un lien ?
- Le site virustotal indique-t-il que le nom de domaine vers lequel pointe l'email délivre des fichiers malveillants ?

Nous allons à présent détailler chacun de ces points dans le cas d'un message de spam reçu sur une boîte email personnelle le 28 juillet 2014 : L'email étudié est illustré par la figure 6

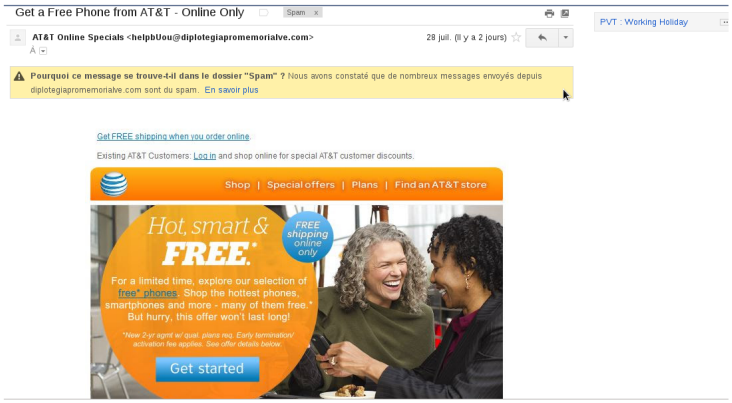

FIGURE 6 – Exemple de courriel malveillant

L'adresse de l'expéditeur est-elle en rapport avec l'adresse d'envoi ? Le logiciel de messagerie permet de connaitre l'emetteur supposé de l'email. Dans ce cas, comme illustré par la figure 7, il apparait que l'entité expéditrice du message est AT&T (il s'agit de *AT&T Online Specials*) ; cependant le nom de domaine utilisé lors de l'envoi du spam est *diplotegiapromemorialve.com*.

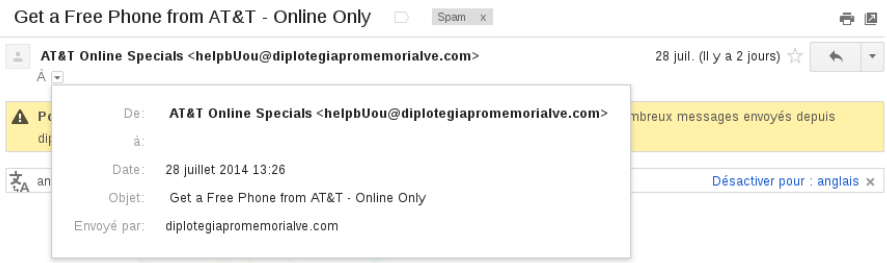

FIGURE 7 – L'adresse expéditeur n'est pas en rapport avec l'adresse d'envoi

Un tel schéma est caractéristique d'un spam. Dans ce cas, l'organisation criminelle à l'origine de la campagne de spam a détourné le serveur dont le nom de domaine est *diplotegiapromemorialve.com* et l'utilise comme relais pour envoyer ses courriers électroniques malveillants. *diplotegiapromemorialve.com* n'était pas forcément visé formellement, mais dans la mesure où son système était vulnérable, il a été pris pour cible afin de mettre ses ressources à disposition de l'entité criminelle, comme expliqué dans la partie 4.4.3.

Indice : L'adresse expéditeur AT&T Online Specials helpbUou@diplotegiapromemorialve.com n'est pas cohérente

L'adresse du destinataire est-elle bien mon adresse ? Le logiciel de messagerie permet de connaitre le destinataire supposé de l'email. Dans ce cas, il n'apparait aucune adresse email de destination. Cela peut être dû au fait que la liste de destinataires est trop importante, ce qui est caractéristique du cas des spams !

Indice : L'adresse destinataire n'est pas mon adresse

Le message m'est-il personnellement destiné ? Le message n'est pas du tout personnalisé ; il n'y figure aucun nom, ou prénom ; rien qui puisse indiquer que ce message avait bien pour destinataire la personne qui l'a reçu. Il peut être envoyé à plusieurs centaines de milliers de personnes sans modification du contenu.

Indice : Un email envoyé lors d'une attaque de masse n'est jamais personnalisé

Le contenu de l'email est-il une image avec un lien ? En passant la souris sur le contenu de l'email, on s'aperçoit en fait que le contenu même de l'email est en réalité une image qui pointe vers une page web `http://diplotegiapromemorialve.com/88VtssVPAjTIM9yL8ol9_h3OP8Y` pour laquelle le nom de domaine *diplotegiapromemorialve.com* est différent de celui attendu (dans notre cas le site officiel d'AT&T)

Ce lien signifie en fait que l'organisation cybercriminelle à l'origine de l'envoi a pénétré le système du serveur hébergeant le nom de domaine *diplotegiapromemorialve.com* et y a déposé un contenu malveillant à l'adresse *diplotegiapromemorialve.com/88VtssVPAjTIM9yL8ol9_h3OP8Y*. Une fois de plus *diplotegiapromemorialve.com* n'était pas forcément visé formellement, mais dans la mesure où son système était vulnérable, il a été pris pour cible afin de mettre ses ressources à disposition de l'entité criminelle ; il s'agit donc d'une illutration du point étudié dans la partie 4.4.1.

Indice : Un email dont le contenu est une image qui possède un lien pointant vers un nom de domaine différent du domaine officiel de l'expéditeur de l'email est très suspicieux !

Le site virustotal indique-t-il que le lien ou le nom de domaine vers lequel pointe l'email délivre des fichiers malveillants ? VirusTotal est un site web qui permet une analyse rapide des fichiers et des URL en les soumettant à une liste de près de 70 antivirus du marché et en retournant le résultat de l'analyse pour chacun d'entre eux.

Proposer l'URL d'un site à virustotal permet donc de se faire une idée assez rapidement de la dangerosité du site en question. Cependant, comme nous l'illustrerons dans la partie 5, cet indicateur à lui seul ne permet pas discriminer une URL malveillante.

Voilà une liste de points qui permettent de classer sans trop se tromper un email dans la catégorie spams ; c'est son caractère massif, global et non personnalisé, voire grossier dans son contenu (une simple image pointant vers un site illégitime) qui nous met la puce à l'oreille. Il est l'exemple parfait d'une attaque non ciblée ; par contre la donne est bien différente dans le cas d'une attaque ciblée.

3.1.2 Un exemple de l'attaque ciblée : le Spear Phishing

La sécurité des protocoles emails Le protocole *Simple Mail Transfer Protocol* (couramment utilisé avec l'acronyme SMTP)[37], défini au début des années 80, est toujours le protocole utilisé aujourd'hui pour l'acheminement des emails. A la date de sa conception, les connexions étaient rares, peu fiables et le premier souci était d'assurer un transport sans perte, ce qui explique que le protocole a été construit avec un effort sur l'aspect fonctionnel mais sans aucune sécurité. Il est par conséquent aujourd'hui possible de forger des emails de toutes pièces en modifiant à souhait l'adresse expéditeur, usurpant ainsi l'identité de qui bon semble.

Les protocoles POP [42] et IMAP[40] permettent de récupérer les courriers électroniques sur les serveurs de messagerie. Egalement définis dans les années 80, ces protocoles n'ont pas été conçus dans un contexte où la sécurité était un enjeu aussi important qu'aujourd'hui. Dès lors, les mécanismes d'authentification, lorsqu'ils sont utilisés, peuvent facilement être déjoués et les contenus des messages peuvent même être modifiés lors de la récupération des messages.

Ainsi, l'intégrité et l'authentification d'un email ne peuvent a priori pas être assurés et nécessitent donc l'ajout d'une couche cryptographique. Effectivement, seul un message signé à partir d'une clé privée non compromise permet de s'assurer à la fois de l'intégrité du message et de son authentification. Cependant, la mise en place d'infrastructures de clés publiques pose un certain nombre de questions qui sont bien au delà du cadre de ce travail mais qui font de cette alternative une solution très imparfaite.

Des raisons historiques permettent donc de comprendre pourquoi un email reçu aujourd'hui dans une boîte aux lettres électronique ne peut a priori pas être fiable, quelles que soient les adresses expéditeurs, ou même le contenu.

Le spear phishing Un email de *spear phishing* est un email semblant provenir d'une personne ou d'une entreprise connue de la victime mais qui a en réalité été envoyé par des personnes ou programmes malveillants. Les faiblesses des protocoles email sont donc utilisés par le cybercriminel afin de falsifier les adresses d'émission et ainsi usurper l'identité du contact de la victime. Dans la mesure où le contenu de l'email est particulièrement ciblé (et s'il est bien conçu), il est beaucoup plus difficile de déceler son intention malveillante ; il peut alors passer complètement inaperçu.

Un email de spear phishing peut par exemple faire référence à des éléments récupérés par la technique de *social engineering* et qui s'intègrent complètement

dans le contexte de la victime afin que celle-ci soit encouragée à suivre un lien ou à ouvrir une pièce jointe piégée. Qui pourrait en effet refuser d'ouvrir la pièce jointe d'un email *provenant* de son superieur hiérarchique et contenant la version signée d'un contrat client ?

Règle 6 : Un email, à moins d'être signé par un protocole cryptographique, ne peut jamais être réputé fiable

Dans la plupart des cas (bien que cela puisse suffire dans certains cas très particuliers –en exploitant par exemple une vulnérabilité du logiciel de messagerie dans le rendu de l'email [130]), la lecture à elle seule de l'email ne va pas compromettre le système de la victime. Celle-ci devra en effet enchainer une combinaison d'actions qui permettront à la charge active de s'activer.

Il apparait par conséquent concevable, au terme de cette introduction aux attaques, d'adopter certains comportements simples afin d'éviter les attaques non ciblées, en tirant profit de leur caractère massif et non spécifique. Une externalité largement positive s'exprime dans le fait qu'en adoptant un tel comportement éclairé, les attaques ciblées, plus complexes à déceler, pourront elles aussi être évitées ou, du moins, leur effet pourra être amorti.

Nous allons donc chercher à comprendre les différents mécanismes de compromission des systèmes afin de repérer les zones et comportements à risques, et d'en déduire le guide d'hygiène comportementale qui en découle.

3.2 Les modes de pénétrations et les règles d'hygiène associées

3.2.1 Modèle formel d'une attaque

L'activation de la charge active Une attaque consiste toujours formellement à lancer une portion de code exécutable qui contient des instructions malicieuses ; ces instructions dépendent fondamentalement du but de l'attaque (les instructions pour une opération d'espionnage seront par exemple différentes des instructions utilisées pour une opération de sabotage). La portion de code qui contient ces instructions s'appelle le *payload* et est dépendante de l'architecture de la machine sur laquelle il s'exécute.

Le *payload* est soit directement contenu dans un fichier binaire que l'utilisateur exécute sur sa machine, soit il est chargé en mémoire et exécuté depuis un code malveillant tirant profit d'une vulnérabilité du système, ou d'une application du système.

Règle 7 : Il y a schématiquement 2 manières d'être infecté :
- En lançant soi-même un fichier exécutable contenant une portion de code malicieux
- Parcequ'un code malicieux exploite une faiblesse dans un système ou une application qui lui permet de charger en mémoire et d'exécuter un *payload*.

De la vulnérabilité à l'exploit Une vulnérabilité dans un système, ou une application, est une faiblesse qui permet à un code malveillant de porter atteinte à l'intégrité du système ; ce code malveillant, qui tire profit de la vulnérabilité, s'appelle un exploit. Son objectif est de parvenir à charger en mémoire et à exécuter un programme, le *payload*, afin de mener à bien l'attaque. Le *payload* permettra alors selon le but de l'attaque soit de prendre la main sur le système compromis, soit d'ouvrir un canal vers un système de contrôle, soit par exemple d'ouvrir une porte dérobée dans le système...

Toutes les applications sont visées par les chercheurs de vulnérabilités, depuis les applications systèmes jusqu'aux applications tierces, depuis le navigateur web, les plugins du navigateur, jusqu'au lecteur pdf ou encore les logiciels de bureautique. A chaque fois, l'attaquant cherche un moyen de détourner à son profit le comportement normal de l'application.

Le jeu du chat et de la souris Une partie des vulnérabilités découvertes sont rendues publiques et *patchées* plus ou moins rapidement. A chaque fois qu'une vulnérabilité devient publique, toute la communauté *underground* s'en empare et l'utilise comme une nouvelle flèche à son arc, développant alors des exploits autour cette vulnérabilité. Il sagit donc d'une course contre la montre pour que les systèmes des utilisateurs soient *patchés* avant que des exploits soient mis en libre circulation et utilisés à grande échelle. Tant que le système n'est pas patché, il est en effet vulnérable, comme l'illustre la figure 8

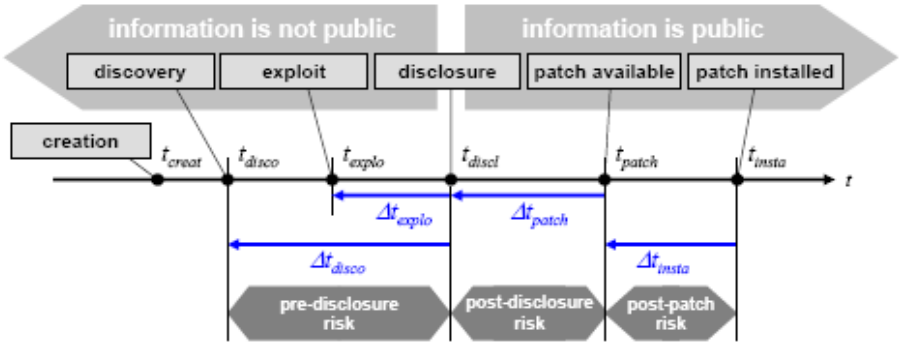

FIGURE 8 – Le cycle de vie d'une vulnérabilité définie par des phases distinctes. La séquence exacte des événements varie selon vulnérabilités.[133]

La figure 9 illustre la rapidité relative avec laquelle les vulnérabilités publiques sont *patchées* par les éditeurs compte tenue de leur divulgation. On s'aperçoit alors que certaines vulnérabilités ne sont *patchées* par les éditeurs que longtemps après leur découverte et le développement d'un exploit relatif, mettant ainsi les systèmes en défaut et faisant d'eux des cibles vulnérables aux attaques.

Si les vulnérabilités ne sont pas rendues publiques, certaines organisations malveillantes tentent d'analyser les mises à jour de sécurité proposées par les éditeurs de logiciels afin de détecter par la méthode de *reverse ingineering* la

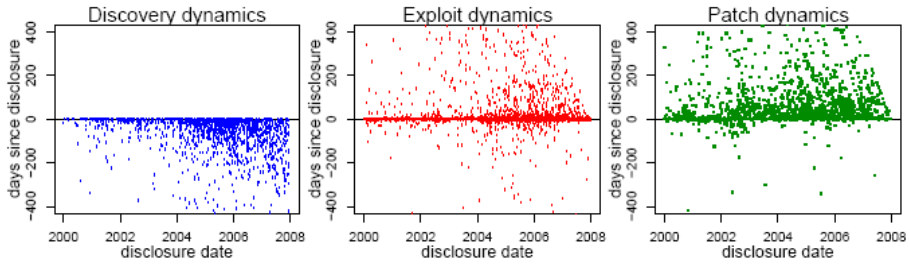

FIGURE 9 – Nuage de points illustrant les temps de découverte de la vulnérabilité (à gauche), disponibilité d'un exploit (au centre), et disponibilité du patch (à droite) par date de la divulgation[133]

portion corrigée et d'en déduire l'endroit de la vulnérabilité. L'objectif est ensuite d'attaquer les systèmes qui n'ont pas été mis à jour.

Les 0-days Il existe enfin certaines sociétés spécialisées dans la découverte de *0 days*, c'est à dire de vulnérabilités non publiques. En France par exemple, la société *Vupen* [20] analyse de manière précise le fonctionnement des applications et systèmes afin de trouver de nouvelles vulnérabilités ; il développe ensuite le code nécessaire à leur exploitation, avant de vendre l'exploit à ses clients.

La figure 10 illustre et synthétise les différents protagonistes intervenant dans cet écosystème.

Une fois assimilé le modèle formel d'une attaque et les rôles des différents protagonistes de l'écosystème, nous allons à présent étudier différentes familles de méthodes d'intrusion fréquemment utilisées pour gagner accès sur un système ; dans chaque cas une règle viendra énoncer le comportement que l'utilisateur doit adopter s'il souhaite réduire la surface d'attaque et donc le risque associé.

3.2.2 Le Drive by download

Principe général Le *drive by download* est le processus par lequel le composant malveillant d'une page web exploite une vulnérabilité du navigateur de la victime, afin d'y charger puis exécuter un *payload* lors de la simple visite d'une page web. L'utilisateur, simplement en visitant un site web se retrouve ainsi piégé. Le schéma d'infection est illustré par la figure 11.

Illusation par l'exemple : Flashback Une illustration de cette famille d'infection peut être trouvée dans l'analyse de l'attaque *FlashBack* qui a compromis plus de 600 000[38] systèmes Apple en exploitant une vulnérabilité dans la machine virtuelle Java [6], rappelant ainsi au passage que les ordinateurs Apple sont bien loin d'être épargnés par ce type d'épidémie.

6. Exploitation des vulnérabilités java CVE-2012-0507 et CVE-2011-3544

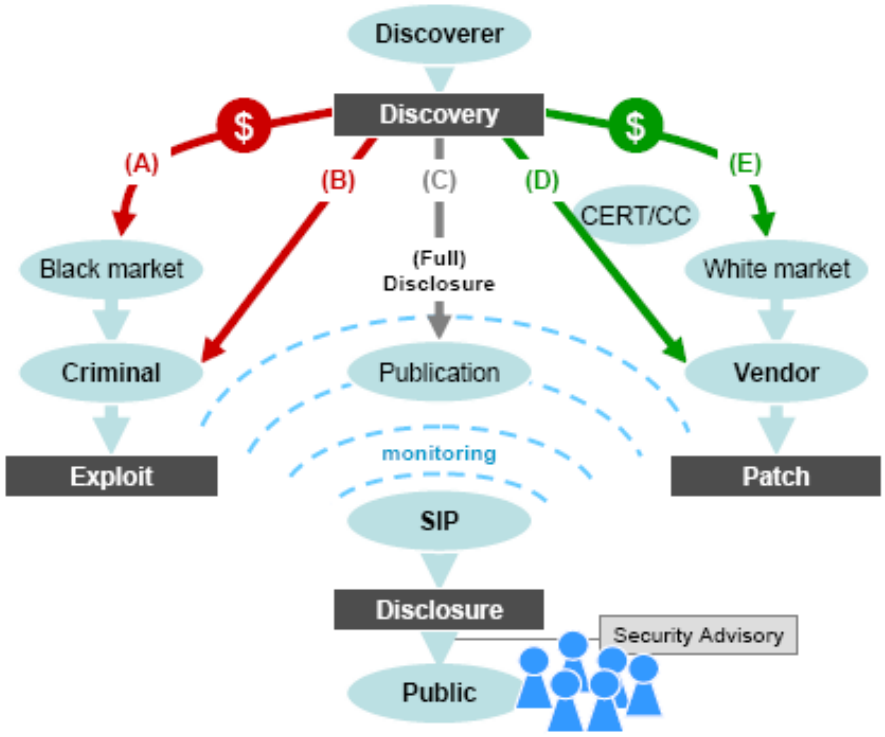

FIGURE 10 – Principaux processus de l'écosystème de la sécurité et relation avec les événements afférents au cycle de vie de la vulnérabilité.[133]

L'industrialisation de ce type d'attaque : multiplier les relais de diffusion Par ailleurs, les attaques modernes mettent en place de véritables plateformes qui hébergent des centaines d'exploits pour un large spectre d'applications et de versions de telle sorte que l'exploit sélectionné et renvoyé au client lors de sa navigation dépend de l'exacte version de son application. Un tel processus permet ainsi de s'assurer d'un taux de pénétration plus important.

Il est par ailleurs assez intéressant de noter que la plupart des sites distribuant des malwares sont en fait des sites légitimes dont les systèmes ont été compromis. En effet, 82 % des site fournissant des malwares sont en fait des sites légitimes contaminés, d'après une étude Sophos[150], nouvelle illustration du principe cité dans la partie 4.4.3, P50.

Parmis les cas les plus tristement célèbres de sites *de confiance* distribuant des *malwares*, on peut par exemple citer *bank of India*[76] ; en 2007, l'institution a alors diffusé des logiciels malveillants et ainsi participé à la contamination des systèmes de ses clients pour le compte d'une organisation criminelle.

Un tel scénario peut ainsi tout à fait expliquer une partie de la compromission des machines d'internautes surfant sur le web de manière tout à fait légitime, d'autant plus que ce phénomène est loin d'être isolé. Google a ainsi

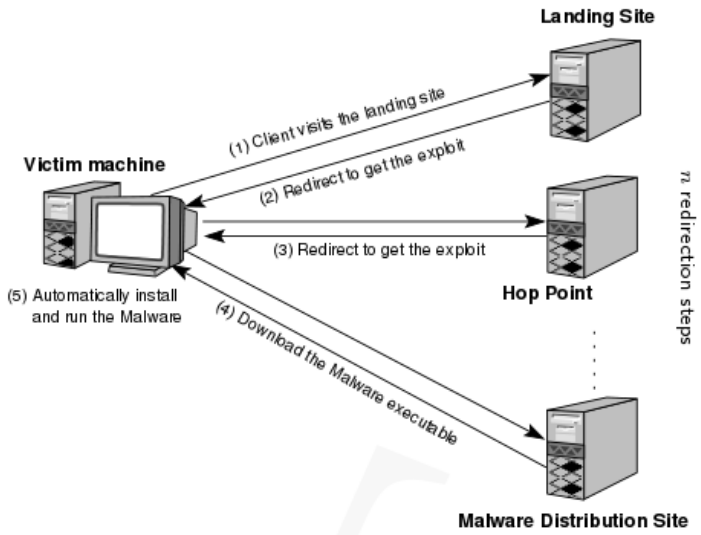

FIGURE 11 – Schéma typique d'un cas de *drive by download.*[115]

démontré que plus de 1,3% des requêtes effectuées contenait au moins une URL malicieuse[115], tel qu'illustré sur la figure 12.

La version ciblée : Opération Aurora L'opération Aurora est une opération de cyberespionage chinois de grande ampleur qui prenait pour cible une trentaine d'entreprises américaines telles que Google, Symantec, Rackspace, Acrobat et d'autres[132] ; cette opération a été mise à jour en Janvier 2010. Son mode d'infection consistait à envoyer un email contenant un lien malicieux. Le lien malicieux pointait alors vers une page web dans laquelle un code javascript tirait profit d'une vulnérabilité *0 day* dans le navigateur *Internet Explorer*. Une fois le navigateur compromis, l'exploit téléchargeait et exécutait un *payload* depuis un site internet afin d'installer un accès distant sur la machine[39]. Cet accès permettait alors aux attaquants de voir, créer ou modifier le système de la victime. Il s'agit d'une illustration parfaite des mécanismes du *drive by download*. Quand cette technique est utilisée dans le cas d'une attaque ciblée et qu'elle est combinée au *spear phishing*, elle porte de nom de *watering hole*.

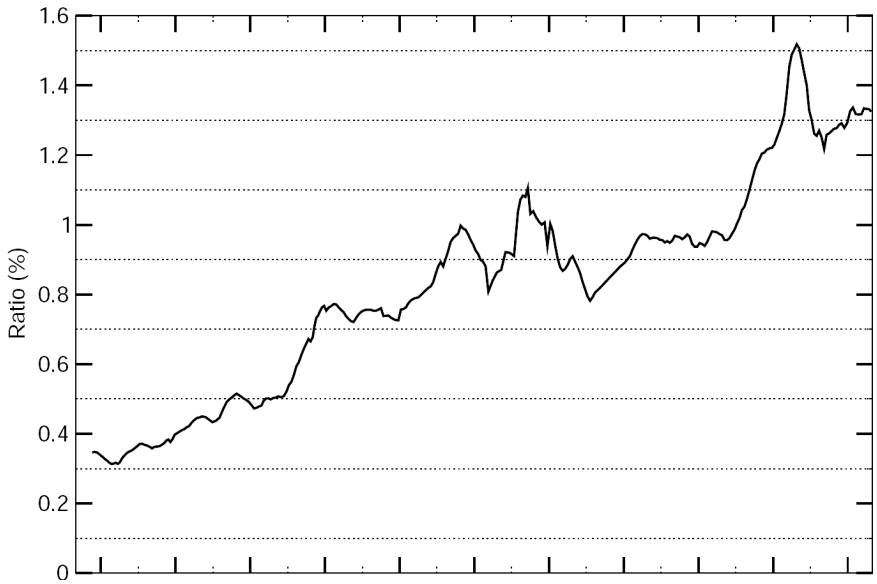

FIGURE 12 – Pourcentage de requêtes sur le moteur de recherche Google dont le résultat retourne au moins une URL d'une page web contenant du code malicieux.[115]

Recommandation 1 : Le meilleur moyen de lutter contre les attaques de type *drive by download* est d'avoir un système systématiquement et rigoureusement à jour [a] (aussi bien le système que l'intégralité des programmes tiers) et de minimiser la surface d'exposition en n'installant que les programmes strictement nécessaires et en n'activant que les modules complémentaires réellement utilisés.

a. Chaque système d'exploitation propose des outils afin de faire des mises à jour de manière automatique

Le cas particulier des Applets Java Les applets java, technique alternative à *Flash*, sont utilisées pour fournir au sein d'applications Web des fonctionnalités interactives qui ne peuvent pas être fournies par le langage HTML. Il s'agit d'un *bytecode* java exécuté sur la machine virtuelle java du navigateur. Étant donné que le *bytecode* Java est multi plate-forme, les applets Java peuvent être exécutées sur différentes plates-formes, dont Windows, Unix, Mac OS et Linux à partir du moment où ces derniers possèdent un plugin java. Le bytecode est exécuté côté client lors de l'affichage de la page web visitée.

Certaines applets java exploitent une vulnérabilité dans la machine virtuelle afin d'être en mesure d'exécuter des commandes directement sur le système. De telles attaques, exploitent régulièrement les vulnérabilités Java[111]. En 2013, c'est par exemple Facebook[86] et Apple[51] qui ont été compromis par de tels moyens. Kaspersky estime aujourd'hui à plus de 90%, la proportion des attaques qui tentent de s'infiltrer dans un système en exploitant une vulnérabilité Java, faisant de cette catégorie un segment à part[96].

Par ailleurs, certaines applets n'essaient pas de tirer profit d'une vulnérabilité du système mais tentent directement d'accéder à certaines ressources protégées. Afin de prévenir des applets qui pourraient souhaiter accéder aux ressources de la machine, les applets java sont exécutés dans un environnement très restreint. Seules les applets qui sont signées cryptographiquement par des tiers de confiance peuvent outrepasser cette sécurité.

Face à cette restriction, les premières applets malveillantes étaient autosignées. Un tel comportement assujétissait donc l'exécution de l'applet à l'accord explicite de l'utilisateur, tel qu'illustré par la figure 13. Une fois de plus, en jouant sur la fonctionnalité, il était alors possible de prendre en otage l'utilisateur et de le *"contraindre"* à exécuter l'applet ; il s'agissait donc de convaincre la victime d'accepter l'exécution d'un code qu'il ne connaissait pas et dont il ne connaissait pas de manière sûre la provenance. . Un tel mode d'emploi a par exemple été utilisé (entre autre [7]) lors de l'attaque FlashBack qui a permis la compromission de près de 600 000 systèmes Apple en 2012[103]

FIGURE 13 – Avertissement préalable à l'exécution du code dans le cas d'une applet non reconnue comme *de confiance*.

Cependant, l'histoire de virus plus récents démontre que désormais, les applets malveillantes utilisent les canaux de certifications habituels afin d'éviter la phase d'avertissements de sécurité de la part du navigateur[77][131] et donc s'exécuter de manière complètement transparente.

Il convient donc de désactiver java dans son navigateur.

7. d'autres méthodes comme la mise à jour d'un plugin java ou l'exploitation d'une vulnérabilité dans le navigateur ont également été utilisées

Recommandation 2 : Il convient de désinstaller Java, vecteur d'intrusion particulièrement utilisé.

3.2.3 Client side exploit

Nous venons de voir comment la simple navigation sur un site légitime compromis qui héberge un code malveillant pouvait mettre à mal l'intégrité d'un système. De même, l'ouverture d'un document, suivant une logique similaire, peut conduire à la compromission d'un système.

Principe Général Lorsqu'elle affiche un document, l'application bureautique doit utiliser une quantité importante de librairies afin de parser et interpréter le code source du document et enfin l'afficher. Or, il se peut que lors du process du document, certaines librairies contiennent des vulnérabilités qui permettraient à un document malicieux, forgé spécialement, de contourner les mesures de protection afin d'exécuter des instructions illégitimes et donc, sous certaines conditions, de prendre le contrôle de la machine.

Dans un tel cas, exploit et *payload* sont insérés directement dans le document, de telle sorte que, lorsque le logiciel est lancé pour afficher ce dernier, l'exploit charge et d'exécute directement le *payload*, rendant en apparence la main au logiciel de bureautique afin de ne pas attirer l'attention de l'utilisateur.

De telles failles sont par exemple assez nombreuses sur le logiciel Acrobat Reader[5],pourtant *reader* par défaut pour afficher les fichiers au format pdf avec de nombreux systèmes d'exploitation ou sur le logiciel Java. En 2013, c'est ainsi 2% des attaques au niveau mondial qui ciblaient le logiciel acrobat reader.

Illustration par l'exemple : attaque du Ministère des Finances Dans le cas d'une attaque ciblée, il suffit donc d'envoyer un email en usurpant l'identité d'un émetteur de confiance tout en incitant fortement la victime à ouvrir le document piégé.

C'est par exemple cette technique qui a été utilisée lors de l'attaque informatique de grande ampleur menée contre Bercy[52] et rendue publique en mars 2011. Des emails, en provenance de personnes de confiance dont l'identité aurait été usurpée ≪ contenaient un fichier [PDF] attaché accompagné d'un message du genre : *regardez ce document, il pourrait vous intéresser*≫ [8]. Une fois ouvert, le document (qui était en réalité un cheval de Troie) exploitait une vulnérabilité dans le logiciel Acrobat Reader qui permettait ainsi de prendre le contrôle du système dans le but d'exfiltrer des documents sensibles.

Ce cas est cependant très loin d'être isolé puisque le rapport de Symantec MessageLabs 2010, stipule que les fichiers PDF piégés sont utilisés dans près de 65% des attaques ciblées[136], tel qu'illustré par la figure 14.

8. Patrick Pailloux, directeur général de l'ANSSI au moment de l'attaque contre Bercy

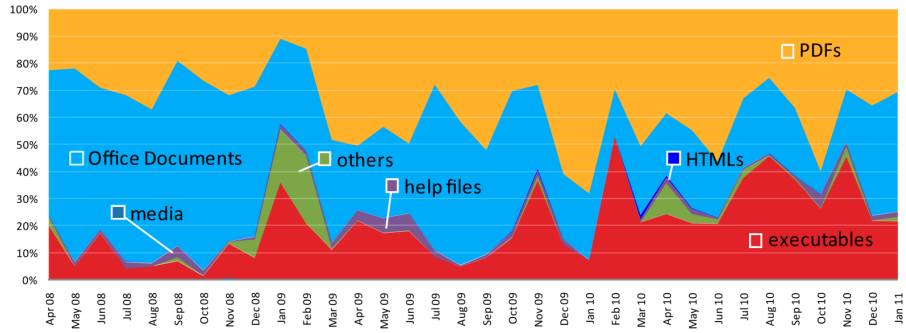

FIGURE 14 – Répartition des types de fichiers malveillants en fonction du temps[136]

3.2.4 Les clés USB

Le principe d'une clé USB Une clé USB est un périphérique de stockage amovible branché sur le port *Unified Serial Bus* d'un ordinateur. La clé USB est composée d'un connecteur USB et d'une mémoire dite *flash*, c'est à dire une mémoire de masse à semi-conducteurs, non volatile et réinscriptible.

De par sa petite taille adaptée au transport, l'absence d'éléments mécaniques qui lui confère une grande résistance aux chocs, une capacité de stockage de plus en plus importante (habituellement quelques giga octets et jusqu'à un téra octets) et la généralisation de l'interface USB, la clé USB est devenue le périphérique de référence pour transférer des données entre systèmes.

Cependant, son universalité en a fait une cible des organisations criminelles qui ont vu en elle un formidable outil d'intrusion ou de vol de données et mis au point des méthodes astucieuses afin de tirer profit de ses potentialités. Nous détaillons ici quelques unes des attaques les plus courantes.

Exécution automatique à l'insertion d'une clé Le fichier *autorun.inf*, situé à la racine de la clé USB, est un fichier texte permettant de configurer un *autorun* pour les systèmes d'exploitation de type Microsoft Windows, c'est à dire, en d'autres termes, permettant de configurer l'automatisation du lancement de certains programmes lors de l'insertion du périphérique, dans une logique *plug and play*.

Il est par exemple possible au travers de ce fichier de fixer un nom à la clé USB et de personnaliser son icône sur le bureau ou encore de spécifier le programme à exécuter lors de l'insertion de la clé, comme le montre l'exemple proposé ci-dessous [4].

```
[autorun]
open=Filename_x86.exe
icon=IconFile.ico
```

Cette fonctionnalité a cependant rapidement été détournée et le paramétrage du fichier *autorun.inf* a permis aux organisations criminelles de lancer l'exécution d'un programme malveillant, une fois la clé insérée et à l'insu de l'utilisateur.

Dans un contexte de contamination, le système compromis, dès qu'il détecte l'insertion d'un périphérique amovible, duplique sur ce support son code malicieux et modifie le fichier *autorun.inf* de telle sorte que le support amovible, contaminé, va diffuser la contamination auprès de tous les nouveaux systèmes sur lesquels il est inséré.

La réponse de Microsoft Face à une menace grandissante, la première parade de Microsoft a été de ne plus permettre l'exécution des *autoruns* depuis les clés USB ; cette modification a été apportée par Windows XP SP2 [12].

Dès lors c'est le mécanisme d'*Autoplay* qui a pris le relais. L'*autoplay* est une fonctionnalité qui permet à l'utilisateur de paramétrer les applications locales à démarrer lors de l'insertion d'un périphérique, en fonction du format des fichiers contenus par le périphérique. A la différence de l'*autorun*, ce comportement est configuré sur la machine et lance des programmes en local donc a priori de confiance.

Une des limites de l'autoplay Cependant, lors du processus de l'*autoplay*, le fichier *autorun.inf* est tout de même parsé afin de proposer des commandes additionnelles qui seront affichées à l'utilisateur dans une boite de dialogue. Il devient alors possible pour une personne malveillante de proposer un programme additionnel, malveillant, pour lire le contenu des fichiers, tel qu'illustré par la figure 15

Exploitation de cette limite, illustration par l'exemple de Conficker C'est par exemple un des moyens de diffusion utilisés par les programmes malveillants de la famille Conficker. Ainsi dès que le périphérique est inséré sur une station compromise, le logiciel malveillant copie l'exécutable malicieux sur le périphérique et modifie le fichier *autorun* présent sur la clé ; il ajoute alors comme option le lancement du fichier exécutable nouvellement copié. Afin de tromper l'utilisateur, le programme malveillant tente même de reprende les codes graphiques de l'explorateur fichier de Windows pour la boite de dialogue [98].

Dès lors, lorsque la clé est par la suite installée sur une station non compromise, l'*autoplay* affiche la liste de possibilité illustrée sur la figure 15. Si l'utilisateur sélectionne le choix par défaut, il lance alors le fichier malveillant qui compromettra son système.

La solution de Windows 7 et ses limites Afin de répondre à ce nouvel aspect, les équipes d'ingénieurs de Windows 7 ont alors modifié le comportement de l'*autoplay* afin qu'il n'intègre plus les configurations apportées par le fichier *autorun.inf* lors de l'insertion d'un périphérique non optique, c'est à dire d'un périphérique type USB.

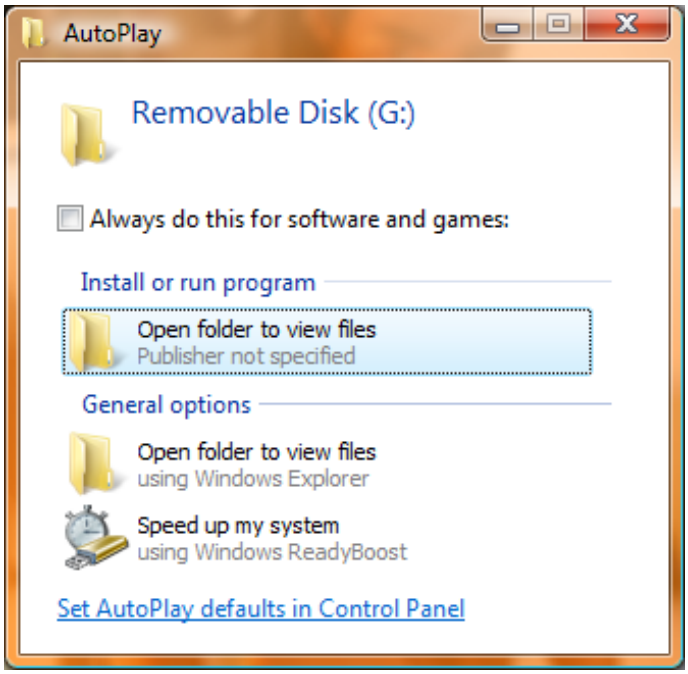

FIGURE 15 – Exemple de l'affichage d'une fonction autoplay trompé par un fichier autorun

Grâce à ce procédé, les virus ne peuvent donc plus se propager par les clés USB en infectant les fichiers *autorun.inf* et en y insérant une commande d'exécution d'un code malicieux.

Cependant, ces contremesures ne concernent en aucun cas les lecteurs optiques de type CD-ROM. Or certains types de clés USB du grand public(par exemple les clés de type U3[147]), pour des raisons *pratiques*, utilisent une technologie qui consiste en une modification logicielle et materielle des clés standards de telle sorte que lorsque la clé est insérée, l'ordinateur perçoit en réalité deux périphériques : un périphérique type CD-ROM qui contient une famille d'applications dites *portables* ou les *drivers* nécessaires au bon fonctionnement de la clé et un périphérique type stockage USB plus classique. Il sera à ce moment là possible de solliciter la fonction *autorun* de Windows dans l'*autoplay* pour la partition CD-ROM.

Or il a été démontré la possibilité, pour certaines clés, de modifier à volonté le contenu de la partie CD-ROM. Dans de telles conditions, il devient donc possible d'y insérer une portion de code malveillant et de changer l'autorun afin de tromper l'utilisateur comme vu précédemment et tel qu'illustré par la figure 15 [53].

Ces vecteurs d'intrusion n'ayant pas été fixés dans les versions de Windows à date, il est fondamental de désativer l'autorun, ou toutes les fonctionnalités

équivalentes sur les autres systèmes d'exploitation

Recommandation 3 : Il convient de désactiver l'*autorun* (ou fonctionnalité équivalente sur les autres systèmes d'exploitation) afin d'éviter tout comportement automatique du système lors de la détection d'un nouveau périphérique.

Exploiter l'Autoplay Tel que décrit dans le paragraph précédent, l'*autoplay* consiste à reconnaitre le format des fichiers présents sur la clé et lancer automatiquement un programme présent sur le système qui puisse lire ce format. Par exemple, si le fichier est un *raccourci* (format *LNK*), c'est l'explorateur Windows qui est lancé, si le fichier est un fichier mp3, c'est le lecteur musique par défaut qui est lancé.

Une famille d'attaques consiste donc à positionner sur la clé un fichier malveillant qui contient intrinsèquement le code d'exploitation d'une vulnérabilité présente dans le programme lancé.

Illustration par l'exemple Ce système était par exemple la méthode d'infiltration retenue par le vers *Stuxnet* [146] afin de pénétrer des environnements indépendants et autonomes, c'est à dire non reliés à internet. Le vers exploitait alors une vulnérabilité *O day* de l'explorateur Windows au moyen d'un fichier *LNK* (type raccourci windows) vérolé.

Par ailleurs, il s'agit surement là d'une des méthodes d'infection préférées lors d'attaque d'espionnage ; des clés USB malveillantes commerciales sont alors offertes ou oubliées négligemment dans un parking et permettent une fois qu'elle sont insérées dans un système de pénétrer ce dernier. Une étude orchestrée par département de la sécurité nationale américaine a d'ailleurs démontré que près de 60% des employés qui trouvent une clé USB dans le parking la branchent sur le PC de l'entreprise. Cette proportion monte à 90% si la clé USB arbore le logo de l'entreprise [60].

Recommandation 4 : Il convient de désactiver l'*autoplay* (ou mécanisme équivalent sur les autres systèmes d'exploitation)afin d'éviter tout comportement automatique du système lors de la détection d'un nouveau périphérique.

Des clés actives La tendance actuelle, et ce depuis quelques années, se dirige vers un *plug and play* généralisé ; l'idée est que tout soit accessible immédiatement une fois l'outil branché. C'était d'ailleurs le sens de l'*autorun* et de l'*autoplay*. Le fonctionnement clés USB sont une belle incarnation de cette volonté d'immédiateté, et l'on a vu dans les paragraphes précédents comment ces automatisations pouvaient être dévoyées par des groupes criminels.

Par ailleurs, les ports USB se sont largement démocratisés et ne sont plus du tout aujourd'hui réservés aux périphériques de stockage de données. Les claviers et souris, par exemple, sont connectés au système via un port USB. Il est question dans cette nouvelles famille d'attaques à base de clés USB d'exploiter cette universalisation.

Certains chercheurs ont démontré qu'il était possible de modifier matériellement et logiciellement une clé USB afin que, une fois branchée sur un système, celle ci se fasse passer pour un clavier[19]. Une fois reconnue comme un clavier, il lui devient donc possible de communiquer avec le système en lançant une invite de commandes et en saisissant les commandes à exécuter, tout ça de manière complètement transparente pour l'utilisateur.

Recommandation 5 : Les clés USB insérés dans les systèmes de l'entreprise doivent être la propriété de l'entreprise et ne doivent en aucun cas venir de l'extérieur ou avoir été branchées sur un système étranger.

Copie du contenu de la clé En outre, il est très fréquent d'utiliser ses périphériques USB sur des systèmes étrangers afin de transférer des données. Lors d'une exposition à l'exterieur par exemple, afin de copier le contenu de sa présentation sur une clé USB et ainsi pouvoir bénéficier des infrastructures mises en place pour la démonstration.

Or, il est possible de modifier les règles de son système afin que lorsqu'un périphérique y est inséré, le système lance une copie bit à bit de l'intégralité du contenu de la clé[**?**]. Ainsi, ce n'est pas seulement le contenu de la clé que l'on est capable de retrouver ulterieurement sur cette copie, mais le contenu de l'intégralité des fichiers qui ont été présents sur cette clé, et ce, même si la clé a été formatée.

Cela est rendu possible par le fait que lors de l'effacement d'un fichier, pour des questions de performances, le fichier en tant que tel n'est pas détruit sur le périphérique de stockage ; seuls sont détruits les pointeurs vers ce fichier dans la table d'indexation, le fichier restant physiquement intact sur la clé.

Recommandation 6 : Les clés USB doivent impérativement être chiffrées.

3.2.5 Utilisation de macro

Certains logiciels de bureautique viennent avec des fonctionnalités avancées qui permettent la mise en place de macros, ou de scripts afin d'automatiser certaines tâches et de gagner en productivité. Il devient alors possible pour une personne mal intentionnée d'ajouter au document légitime un script qui s'exécute au lancement de l'application afin de prendre la main sur le système.

Des logiciels de bureautiques appartenant à la suite *Microsoft Office* comme *Word* ou *Excel* permettent par exemple la création de macro à l'aide du langage VBA, alors que le logiciel *Acrobat Reader* permet l'exécution d'animations *Flash* ou de scripts *Javascript*.

Depuis quelques années, la suite *Office* exige alors qu'une permission soit donnée explicitement par l'utilisateur avant d'autoriser l'exécution de macro. Cependant, une fois de plus, le besoin d'immédiateté (étudiée dans la partie 1.3.2, P12) dans l'accès à la fonctionnalité conduit l'utilisateur à des choix non raisonnables.

3.2.6 Direct download (fake av, plugin, addon)

Enfin, il est fréquent que l'utilisateur cherche lui-même à installer un programme sur son système, sans forcément se douter que ce programme est malveillant. Il existe une quantité importante de tels programmes.

On appelle cheval de Troie un "programme donnant l'impression d'avoir une fonction utile, mais qui possède par ailleurs une fonction cachée et potentiellement malveillante" [9][7].

" [...] Le seul moyen dont dispose le cheval de Troie pour s'installer dans un système est de ... demander de l'aide à l'utilisateur, en lui proposant une action qui semble anodine comme un simple "clic" "[55].

En pensant installer un programme utile pour son système, l'utilisateur installe en réalité également un programme malicieux qui permettra de prendre la main sur tout ou partie de son système. De tels logiciels malveillants peuvent être véhiculés par des vecteurs protéiformes :

Plugins Un des moyens actuels les plus répandus pour prendre la main sur un système consiste à demander à l'utilisateur d'installer ou de mettre à jour un plugin pour son navigateur, tel qu'illustré par la figure 16. L'idée est la plupart du temps de prendre l'utilisateur en otage en arguant que la fonctionnalité recherchée dépend de l'installation ou de la mise à jour de cet add-on. Dans la mesure où la nécessité d'immédiateté dans l'obtention d'une fonctionnalité prime de nos jours toujours sur la sécurité (voir 1.3.2, P12), l'auteur de l'attaque a de grandes chances que l'utilisateur installe le bout de logiciel.

Il s'agit alors pour lui d'insérer dans un plugin légitime une partie de code malveillant qui lui assure le contrôle du système cible ; ce genre d'attaque est quelquefois repéré par les équipes de Mozilla[114].

9. Définition ANSSI

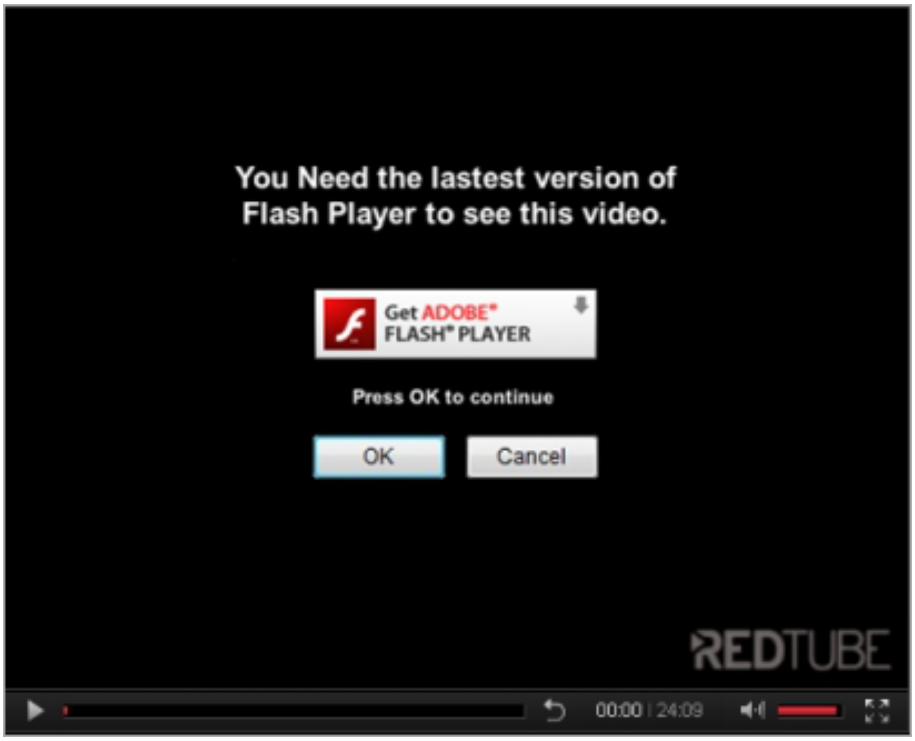

FIGURE 16 – Le site web demande la mise à jour de Flash pour pouvoir lancer la vidéo.

A date d'écriture de ce rapport, c'est probablement les plugin flash et java qui sont les plus utilisés dans ce genre d'attaque. Présents sur la plupart des navigateurs, de tels pluggins permettent normalement la prise en charge d'animations lors de l'affichage de pages web.

En arguant le besoin de mise à jour de ce plugin, l'attaquant insère en réalité un code malveillant sur la machine. Un tel mode d'emploi a par exemple été utilisé (entre autre [10]) lors de l'attaque FlashBack qui a permis la compromission de près de 600 000 systèmes Apple en 2012[103]

Rogues programs D'autres sites encore proposent l'installation de programmes comme des antivirus. En arguant par exemple que le système est infecté, l'auteur malveillant joue sur la peur afin de tenter l'utilisateur pour qu'il installe un nouveau logiciel *"plus efficace"*. L'installation du programme aura en réalité pour conséquence de supprimer les logiciels antivirus existants et de prendre la main sur la machine.

Une liste non exaustive de ce type de programmes pourrait inclure les familles suivantes :

- Antivirus / anti spyware /
- Add block

10. d'autres méthodes comme l'utilisation d'une applet java ou l'exploitation d'une vulnérabilité dans le navigateur ont également été utilisées

– Logiciel de P2P
– Logiciel connu (Flash, Adobe Acrobat Reader, suite microsoft office,...)
– Jeux

Tous les programmes téléchargés Tous les programmes téléchargés depuis internet et installés sur un système peuvent être compromis et contenir en plus du programme légitime une partie de code malveillant. Aussi, il est primordial de ne télécharger les programmes nécessaires que depuis des sources de confiance, c'est à dire les sources officielles. On se gardera par conséquent bien de télécharger et d'exécuter un fichier qui proviendrait d'un site différent du site officiel d'origine du produit.

Par ailleurs, on prendra bien soin de vérifier avant chaque installation que la version du binaire que l'on est sur le point d'exécuter est bien similaire à la version officielle en vérifiant les empreintes cryptographiques des 2 versions. Ces empreintes cyptographiques sont appelées *hash* et sont disponibles la plupart du temps sur le site officiel lors du téléchargement d'un fichier binaire.

La vérification de cette empreinte permet de s'assurer que le fichier que l'on a téléchargé est exactement similaire [11] au fichier officiel et qu'il n'a pas été modifié par un intermédiaire malveillant lors du téléchargement. En effet, le protocole HTTP qui est le protocole de communication de base entre un navigateur web et un serveur, ne permet en aucun cas de s'assurer de l'intégrité du contenu émis ou reçu par un serveur. Il est donc possible sous certaines conditions de modifier les paquets émis par le serveur, en y insérant une portion de code malveillant, avant de les rerouter vers le navigateur client (voir illustration faite à la partie 5.1.3, P53).

Recommandation 7 : On ne télécharge que les applications strictement nécessaires au bon fonctionnement opérationnel de l'activité. Les applications sont exclusivement téléchargées depuis les sites officiels. La vérification des empreintes cryptographiques avant installation du logiciel téléchargé est nécessaire afin de s'assurer que la version téléchargée est bien conforme à la version officielle.

3.2.7 Les réseaux pair-à-pair –P2P

Les réseaux *peer-to-peer*, souvent utilisés dans le but de télécharger des ressources de manière décentralisée, sont une source d'infection particulièrement virulente et ce pour plusieurs raisons :

La qualité des fichiers téléchargés La démocratisation du téléchargement massif de fichiers via les protocoles pair-à-pair a conduit les cybercriminels à utiliser ces canaux afin de diffuser aussi massivement que possible des logiciels malveillants. Dès lors ces logiciels prennent la forme de logiciels légitimes et, lorsqu'ils sont installés sur le système cible permettent en réalité l'exécution de commande malicieuses.

11. avec une probabilité suffisante

En 2008, le rapport de l'antivirus Mc Afee insiste sur l'utilisation de réseaux pair-à-pair pour le téléchargement de films ou de musiques dont les fichiers contiennent en réalité, en plus du contenu désiré, un code malveillant qui au choix exploite une vulnérabilité dans un lecteur vidéo ou s'exécute directement sur le système cible. En pensant télécharger simplement un film, la victime télécharge et exécute en fait un cheval de Troie.

La qualité des programmes de peers-to-peers La qualité instrinsèque du logiciel de P2P est également au coeur des enjeux de sécurité. De fait, de nombreux logiciels incluant des portions de code malicieux sont diffusés de façon étendue en vantant leur caractéristiques techniques supérieures et leur rapidité, un peu à l'image des *rogues programs* étudiés précédemment (voir partie 3.2.6, P43).

L'ouverture de son disque Par ailleurs, le *peer-to-peer* est un paradigme réseau dans lequel chaque système est connecté à une multitude d'autres systèmes. En installant ce type de programmes sur un système, on accepte alors que son système soit connecté avec cette multitude d'autres systèmes que l'on ne connait pas et que l'on ne maitrise pas. Si le logiciel de P2P comporte des vulnérabilités, il devient donc possible de lui faire exécuter depuis le réseau des commandes malicieuses et ainsi de prendre la main sur le système cible.

Recommandation 8 : L'utilisation de réseaux P2P est proscrite.

4 Les conséquences d'une infiltration

Après avoir étudié les vecteurs d'accès les plus répandus lors d'attaques informatiques, il convient à présent de s'interroger sur les différents types de charges malveillantes qui sont activées afin de comprendre, selon les cas, les ressources ciblées par les attaquants. Nous chercherons alors à démontrer que l'intérêt financier est omniprésent et sous-jacent dans chaque attaque. La victime, piégée, sera alors soit dans une position où elle diffuse contre sa volonté des informations confidentielles, soit dans une position où elle perd l'accès à son système d'information. A titre d'exemple, elle peut dès lors soit devenir complice par négligence de l'organisation criminelle en hébergeant des ressources illégales, soit plus simplement être rendue inopérante par la perte d'usage de son système d'information.

4.1 Assurer un revenu

La première des motivations d'une attaque consiste tout simplement à assurer un revenu à l'attaquant.

4.1.1 Ransomware

Un ransomware est une charge malicieuse qui rend inutilisable le système d'information de la victime. Il s'agit d'une "forme d'extorsion imposée par un code malveillant sur un utilisateur du système. Si ce dernier refuse de payer ou d'effectuer une tâche imposée, le service auquel il veut accéder lui est refusé par le code malveillant."[7]

Pour prendre un exemple concret, le logiciel malveillant connu sous le nom de *Crypto Wall Decrypter*[69] fait son apparition en Juillet 2014 ; sa propagation est assurée par le biais d'une attaque de *phishing*.

L'email contient en pièce jointe, un fichier zip qui contient un agent de chiffrement. Une fois qu'il est activé, cet agent va chiffrer l'intégralité du disque dur de la victime à l'aide de l'algorithme de chiffrement asymétrique RSA2048. Le déchiffrement est alors assujéti au paiement d'une rançon dont le montant est fonction du nombre de fichiers chiffrés.

L'utilisateur se retrouve ainsi pris en otage et perd complètement l'accès à son système d'information. Des logiciels malveillants de ce type sont envoyés lors d'attaques massives et peuvent notamment être hébergés sur des sites web compromis ou véhiculés par les réseaux pair-à-pair comme étudié précédemment.

Recommandation 9 : Effectuer des backups réguliers de son système est une bonne pratique.

Un scénario assez proche consiste à activer les micro et webcams de ses victimes, afin d'enregistrer des scènes de la vie courante afin dans un second temps de faire chanter ses victimes[148].

4.1.2 Extorsion

Une pratique voisine consiste à pénétrer le système d'information d'un agent économique, puis de le contraindre, sous la menace, au paiement d'une rançon, sous peine de diffuser les données souvent confidentielles et sensibles, acquises lors de l'attaque.

L'entreprise Domino's a par exemple été la cible d'une telle attaque ; cette attaque a été revendiquée par le groupe de hackers Rex Mundi au premier semestre 2014 .

Rex Mundi (*"roi du monde"*, en latin) est un groupe organisé de cybercriminels, spécialisés dans le chantage sur internet. Leur méthode consiste à s'infiltrer dans le système d'information d'une entreprise, récupérer des informations confidentielles (soit des données clients/fournisseurs, soit des données opérationnelles) puis d'extorquer les victimes.

Ainsi, Domino's communiquait sur Twitter, ≪*Domino's Pizza France a été la cible d'une attaque informatique sur la plateforme technique qu'elle utilise pour gérer son site commerçant. Cet accès illégitime a potentiellement entraîné la récupération d'un nombre limité de données*≫. Rex Mundi aurait accepté de ne pas diffuser les données personnelles récupérées en échange d'un montant de 30 000 euros.

4.1.3 Click Fraud

Le système publicitaire de paiement au clic (*pay-per-click*) propose à chaque hébergeur d'une publicité (c'est à dire le site web qui affiche la publicité) d'être rémunéré par l'annonceur lorsqu'un visiteur de son site clique sur une bannière publicitaire appartenant à l'annonceur.

Ce modèle permet à de nombreux sites dont des sites importants comme *Facebook* de s'autofinancer sans pour autant faire payer un service aux utilisateurs. En France, au premier semestre 2014, le chiffre d'affaires de ce marché est évalué à 1,440 milliards d'euros[35].

Une des fraudes les plus classiques depuis l'apparition de ce système de rémunération, dit fraude au clic, ou *click fraud*, consiste à faire effectuer par une personne ou de manière automatique les clics sur les publicités de façon à se rémunérer.

Dès lors, l'organisation malveillante peut simuler le clic d'un visiteur sur le lien d'une bannière publicitaire à chaque visite sur un site légitime détourné, de telle sorte que chaque visiteur se connectant sur le site sera source de revenu pour l'organisation criminelle.

De manière parallèle, certains programmes malveillants, comme DNSChanger[84], ont été développés dans le but de rediriger les clics des utilisateurs vers des liens sponsorisés ou vers des sites légitimes au moyen de liens d'affiliation. Les auteurs à l'origine de ce programme malveillant ont dégagé jusqu'à 14 millions de dollars de bénéfices[36].

4.1.4 La porte dérobée

Une porte dérobée est un programme informatique qui permet à l'attaquant de se reconnecter quand il le souhaite sur la machine compromise et d'y exécuter des commandes.

Une porte dérobée permet à un attaquant malveillant de préserver un accès sur un système qu'il a compromis. Dès lors, au moyen de cette porte dérobée (également communément appelée *backdoor*), il sera en mesure de se connecter à nouveau sur le système compromis afin d'y exécuter de nouvelles actions.

Un tel accès sur un système peut se monnayer très cher, l'attaquant se lançant alors dans une entreprise de chantage auprès de ses victimes tel qu'étudié dans la partie 4.1.2.

4.2 Espionnage

Dans le cas d'une attaque de type espionnage les charges activées la plupart du temps sont les keyloggers et les spywares.

4.2.1 Keylogger

Un keylogger est un programme malveillant dont le but est d'enregistrer les frappes tapées au clavier par l'utilisateur. Ainsi, l'opérateur malveillant peut récupérer par exemple les mots de passe et autres données sensibles comme les données bancaires de l'entreprise.

Le keylogger renvoie alors de manière régulière par email ou sur un serveur controllé l'ensemble des frappes tapées au clavier par la victime.

4.2.2 Spyware

Un spyware est un logiciel qui permet de transmettre à des tiers des informations sur les usages habituels des utilisateurs du système par exemple ses données de connexion. Il est également possible par ce biais de transmettre les fichiers contenus sur l'odinateur cible vers l'exterieur.

Un tel processus entraine alors la fuite de la propriété intellectuelle.

Les logiciels se sont d'ailleurs affinés ces dernières années de telles sortes qu'afin de ne pas éveiller les soupçons, les fichiers sont désormais segmentés et envoyés par morceaux au fil du temps, afin de piéger les logiciels de détection d'intrusion.

4.3 Sabotage

La volonté de sabotage nécessite un accès au moins partiel sur le système de la victime. Pour cette raison, l'attaquant prendra soin d'activer une charge qui permettra la mise en place d'une porte dérobée.

L'organisation pourra également développer un programme informatique malveillant qui détruise les parties fondamentales des systèmes afin d'en empêcher le bon fonctionnement. A titre d'exemple, dans le cas AramCo cité précédemment, le virus qui s'est propagé contenait une charge active dont le but était d'endommager le *master boot record*[12] afin de rendre les systèmes inutilisables.

4.4 Utilisation de ressources et conséquences associées

Comme expliqué dans les parties précédentes, des attaques de masse sont régulièrement lancées par des groupes organisés de cyber criminels afin de trouver de nouvelles ressources qui viennent renforcer la résilience et la qualité de leurs plateformes. Ces nouvelles ressources sont en fait dérobées aux utilisateurs sans leur permission.

Nous tentons de lister quelques exemples de la façon dont peuvent être dévoyés des systèmes légitimes mal protégés, une fois qu'ils ont été infectés par des attaques de masse, ainsi que les conséquences de tels détournement pour l'entreprise.

4.4.1 Utilisation du serveur de messagerie de l'entreprise

L'utilisation massive de serveurs de messagerie distribués permet aux cyberattaquants de poursuivre leur activité d'envoi d'emails illégitimes et malveillants. Dans la mesure où les relais de spams sont *blacklistés* dès qu'ils sont identifiés[119], il est nécessaire pour les organisations malveillantes de changer très régulièrement de serveurs d'envoi afin de s'assurer que les emails envoyés seront bien routés jusque dans les boites emails des destinataires et ne seront pas rejetés avant par un logiciel antispam (souvent intégré à l'application email).

Dès lors, de manière continue, des robots scrutent internet à la recherche de serveurs emails faiblement protégés (c'est à dire permettant le relais) ou de systèmes sur lesquels il est possible d'installer un serveur email afin de mettre en place une nouvelle plateforme d'envoi de courriels indésirables.

Le système compromis devient alors la source de l'envoi de spams et d'emails de phishing.

12. Le *mater boot record* est le nom donnée au premier secteur adressable d'un disque dur ; il contient notamment la table des partitions et la routine d'amorçage qui a pour rôle de charger le système d'exploitation. Il est alors utilisé par le *bios* dans les toutes premières étapes du démarrage d'un système et sa compromission rend tout le système inutilisable

Conséquence : Une fois que les serveurs anti-spam catégorisent le serveur email de l'entreprise comme serveur de spam, l'intégralité des emails en provenance de son nom de domaine seront par la suite blacklistés ; l'entreprise perd donc totalement sa capacité à communiquer avec l'exterieur.

4.4.2 Utilisation des systèmes de l'entreprise, l'attaque DDOS

Le principe d'une attaque en déni de service consiste à saturer un système en routant vers lui un nombre considérable de requêtes. La masse de requêtes qui parvient simultanément sur un même système dépassant ses capacités, celui-ci n'est plus en mesure de fonctionner correctement.

Lors de ces attaques, la plupart du temps, un nombre important de machines effectuent à leur insu des requêtes sur le système cible. Ces machines sont appelées des zombis, ou *bot* en anglais. Il s'agit de systèmes compromis qui obéissent alors aux *maitres* des groupes malveillants.

Les groupes de cybercriminels organisés proposent la location de réseaux de machines zombis pour mener à bien des attaques de type Déni de Service. Afin d'être en mesure de fournir des ressources en nombre suffisant, ils sont en permanence à la recherche de nouvelles machines faiblement protégées sur internet, afin de les compromettre et de les rajouter à leurs réseaux.

Les attaques les plus importantes recensées à ce jour atteignent ainsi des sommets, jusqu'à 400Gb par seconde[117], et utilisent comme moyen d'amplification des protocoles standards de l'internet comme le DNS ou le NTP. En 2013, l'organisation de lutte contre le spam *SpamHaus* avait ainsi été prise pour cible d'une attaque de grande ampleur après qu'il a pris la décision de placer sur liste noire les adresses IP liées à un hébergeur réputé pour être très permissif... Cette attaque avait alors atteint jusqu'à 300 GB par seconde[99].

On estime à 150 millions soit près d'un quart, le nombre de machines infectées passées sous un commandement tiers[52].

Conséquence : Lors de l'attaque en dénis de service, toutes les machines *bot* envoient massivement des requêtes vers la victime. Si plusieurs machines d'un réseau d'une PME sont compromises, il est fort probable que l'envoi massif de requêtes depuis ces systèmes sature les liens propres de la PME et rende dès lors ses propres systèmes indisponibles, ce qui peut avoir des conséquences particulièrement importantes sur son activité.

4.4.3 Utilisation des ressources de l'entreprise pour la distribution de contenu illicite

Enfin, les organisations criminelles ont besoin de pouvoir héberger les logiciels malveillants ou tout autre type de contenu illicite de manière distibuée

de telle sorte que le nettoyage d'un système ne perturbe pas la bonne continuité du service de distribution de malwares. Les organisations cybercriminelles cherchent donc à constuire des infrastructures résilientes.

Chaque système compromis et connecté à internet est un très bon candidat pour héberger ces logiciels malveillants et participer à la pérennité de l'entreprise d'infection.

C'est la façon dont fonctionne aujourd'hui une grande partie de l'activité cybercriminelle de masse. Des malwares sont hébergés sur des plateformes compromises et ensuite redistribuées et diffusées vers de nouvelles cibles visitant les pages compromises soit directement soit suite à la réception d'un email malicieux.

Une étude menée par HTTPCS (Hypertext Transfer Protocol Certified Secured), une start-up dont le coeur de métier porte sur la sécurité des applications Web, conclut que 72% des sites web français sont vulnérables. La proportion monte à 80 % sur le *.fr* uniquement[44].

Ainsi, ce n'est pas forcément la donnée intrinsèque de l'entreprise qui est visée, mais parfois juste sa bande passante ainsi que son infrastructure ; l'entreprise devient quelque part coupable de complicité par négligence. Une fois complice, ce n'est souvent qu'une question de temps avant que les services de messagerie, considérés comme relais de spams, ne puissent plus communiquer vers l'exterieur, chaque message recevant alors le label de spam et étant détruit avant même d'arriver jusqu'à la boite mail du destinataire, et que les liens réseau soient saturés par le lancement intempestif d'attaques en dénis de service. Enfin, l'image de l'entreprise en ressort dégradée, et en particulier lorsque la finalité de la prise de contrôle heurte les codes sociétaux, par exemple, lorsqu'elle se retrouve accusée de soutenir l'industrie pédopornographique[149]. De plus, la remise en marche d'un système fonctionnel devient une source de coût important qui peut également mener à un dépot de bilan.

Il apparait donc fondamental de se saisir au plus tôt des questions relatives à la cybersécurité et d'appliquer d'appliquer des mesures graduelles cohérentes selon son niveau d'exposition. Le spectre de celles-ci s'étend des mesures de base évoquées au sein de ce mémoire, à d'autres extensives et rigoureuse lorsque l'exposition de l'entreprise devient importante, en passant par celles d'hygiène informatique proposées par l'ANSSI[46]. Dans tous les cas il est primordial de faire le deuil des idées reçues en matière de cybersécurité, surtout celles présentant des solutions techniques miracles qui proposeraient une protection parfaite.

5 Il n'existe pas de solutions évidentes

Ainsi que nous l'avons démontré dans la partie précédente, si les attaques sont souvent motivées par l'appat du gain, la menace n'en reste pas moins particulièrement protéiforme. Certaines règles ont été enoncées afin d'assainir son comportement sur internet et de proposer une hygiène comportementale élémentaire.

Nous démontrerons dans cette partie que le respect de ces règles est indispensable et qu'il n'existe aucune solution toute intégrée miracle qui puisse à ce jour remplacer un comportement responsable.

5.1 Antivirus - firewall

L'inconscient collectif porte bien haut l'idée que le diptyque antivirus-firewall est un rempart suffisant contre une attaque informatique. Une telle certitude, certainement inculquée par les équipes *marketing* des grandes sociétés d'antivirus, est en réalité néfaste pour l'utilisateur qui dédouanera ainsi son comportement risqué, persuadé de toute façon qu'il sera protégé.

5.1.1 Le paradoxde de l'antivirus

Le paradoxe de l'antivirus porte sur le fait que s'il doit protéger le système sur lequel il est installé, l'antivirus ne doit pas pour autant être trop prolixe, s'il ne veut pas être désinstallé par l'utilisateur agacé de recevoir des alertes récurrentes (quelles que soient d'ailleurs la pertinence des alertes).

Par ailleurs, les utilisateurs sont souvent persuadés que leur système n'est pas compromis, dans la mesure où la compromission n'est pas visible. Ainsi, dans l'inconscient collectif, si l'antivirus ne signale pas qu'il y a un virus, c'est qu'il n'y en a surement pas !

5.1.2 La difficulté d'appréciation

La difficulté d'appréciation vient du fait que l'incident ne peut pas être visible simplement comme ce peut par exemple être le cas dans un incendie ou un cambriolage où des indices visibles permettent rapidement à un esprit humain de converger. Dans le cas d'un système informatique, l'attaque résulte simplement dans l'exécution de commandes tierces sur le système. S'apercevoir qu'une commande malicieuse est exécutée est particulièrement difficile, ne serait-ce que parce que la définition même de malicieuse peut être sujette à interprétation.

En outre, même dans le cas d'un antivirus performant, le besoin d'immédiateté dans l'accès à une fonctionnalité (voir 1.3.2) ou un service conduit souvent l'utilisateur à contourner les alertes et les protections du logiciel.

Enfin, l'antivirus est un programme informatique installé sur un système, en local ; il a pour objet de protéger le système de l'exécution de code malveillant. Il y a des lors une quantité de cas pour lesquels l'antivirus ne peut être une solution adéquate, puisque en dehors de ses domaines de compétences.

5.1.3 Cas d'un Wifi public

Le Wi-Fi est un ensemble de protocoles de communication sans fil. Il permet de s'affranchir de la contrainte physique d'un cable et offre des débits de connexion particulièrement intéressants. Le besoin croissant de mobilité dans les entreprises et la nécessité toujours plus grande de connexion à largement contribué à l'expansion massive de l'utilisation de ces protocoles sans fil, de telle sorte qu'à date d'écriture de ce rapport, les points d'accès sans fil se sont multipliés dans les commerces, cafés, grandes enseignes (Mc Donalds, Quick, ...) et jardins publics[9].

Dans la plupart des cas, ces points d'accès sont dits "Ouverts", c'est à dire que le contenu des paquets internet qui transitent entre le point d'accès et le système utilisateur ne sont pas chiffrés. Dans la mesure où les informations circulent sur des ondes, qui ne sont par principe pas unidirectionnelles, il devient possible pour le *quidam lambda* d'enregistrer et de scruter l'intégralité des paquets échangés sur le réseau ; il lui suffit pour ce faire d'écouter les ondes.

Si des mots de passe sont saisis ou des identifiants de connexion (comme des cookies de session) envoyés, il devient possible pour une personne mal intentionnée de récupérer, sous certaines conditions, ces éléments pour se connecter à son tour sur les applications correspondantes. Aucune compétence technique spéciale n'est requise, des logiciels gratuits étant accessibles directement sur internet.

Par ailleurs, l'attaquant peut par la suite occuper une position de type *man in the middle*, dans laquelle il usurpe l'identité du point d'accès et de la station de telle sorte qu'il devient le relais de toute communication entre les deux machines. Dans ce cas, il lui est possible de modifier au fil de l'eau le contenu de ce qui est renvoyé au client[29]. Il peut ainsi le rediriger vers des pages piégées[41] et dans un second temps prendre la main sur son système.

Dans la mesure où cette attaque n'est pas directement liée au système mais tire profit du fait que le protocole wifi, lorsqu'il est ouvert, ne permet ni la confidentialité, ni l'authenticité ni l'intégrité des données qui sont échangées, un antivirus est parfaitement impuissant face à une telle situation.

Recommandation 10 : L'utilisation de Wifi libre ouvert ou protégé avec le protocole WEP est à éviter. Elle pourra être tolérée si et seulement si :
- Le système est connecté en VPN à un réseau de confiance (réseau personnel ou de l'entreprise)
- Les flux sont dirigés vers un proxy au travers d'un canal sécurisé (type ssh)

Dans tous les cas, on lui préfèrera l'utilisation du protocole WPA2 (ou WPA CCMP) avec utilisation lorsque cela est possible d'un serveur d'authentification Radius (802.1x EAP-TLS).

5.1.4 Démarrage sur un système alternatif

Un antivirus n'est actif que lorsque le système sur lequel il a été installé est en fonction. Or il est possible sous certaines conditions de démarrer un système sur un système d'exploitation alternatif ; le chargement de ce nouveau système peut se faire par un périférique externe, la plupart du temps soit à l'aide d'une clé USB soit d'un disque type CD-ROM.

Le principe d'une telle attaque est de se servir des ressources physiques de l'ordinateur pour faire tourner un système d'exploitation tiers. Dans un tel cas, l'antivirus du système légitime n'est bien sûr pas activé dans la mesure où le système d'exploitation sur lequel il est installé n'est lui-même pas en fonction.

Cependant, le disque dur faisant partie des ressources physiques, il est lui complètement accessible, à la fois en lecture et en écriture. Il est donc possible pour une personne malveillante, de récupérer les informations contenues sur le disque, de modifier certains documents où de s'assurer un accès à long terme sur le système.

Recommandation 11 : Chiffrer l'intégralité de son disque dur est une bonne pratique.

Ces deux attaques particulièrement "basiques" permettent de démontrer que la simple utilisation d'un antivirus ne permet pas de prévenir l'ensemble des menaces. Nous allons à présent tenter de démontrer que le fonctionnement même d'un tel programme ne peut répondre à la question de la sécurité d'une station et alors justifier le propos même de Bryan Dye, vice président de Symantec, qui prétend que *l'antivirus est mort*[33].

5.1.5 Fonctionnement et limites de la détection par signature

Lorsque les chercheurs d'une société antivirus détectent un programme malveillant, ils génèrent une signature, c'est à dire un bout de code censé identifer de manière formelle la variante du programme malveillant nouvellement découverte. Cette signature est ensuite ajoutée à la base des signatures de virus. De manière régulière, les logiciels antivirus présents sur les systèmes se connectent à cette base de signatures et mettent à jour leur version, avec les nouvelles signatures.

Ainsi, la prochaine fois que l'antivirus devra analyser le code malveillant, il en extraira la signature et la comparera avec la liste des signatures qu'il possède sur l'intégralité des logiciels malveillants qu'il connait.

On voit donc ici un premier biais dans la construction même du paradigme de l'antivirus. Celui-ci se base lors de son analyse par signature, uniquement sur la détection de programmes connus. Dès lors, un nouveau programme malveillant, ne peut pas être détecté par cette méthode.

Par ailleurs, les développeurs de programmes malveillants ont développé une quantité d'outils et de méthodes pour que le programme mute lors de chaque infection et ainsi générer à chaque fois un nouveau programme malveillant, unique. Ce faisant, ils peuvent donc flouer les mécanismes de vérification de signatures. Nous exposons ici quelques une de ces méthodes :

Metamorphisme Le chiffrement d'un virus permet de brouiller l'aspect du code chargé en mémoire. Si le virus est systématiquement chiffré avec une clé différente alors l'apparence du virus sera différente à chaque fois. Il est donc impossible de déterminer une signature sur le corps de la charge malicieuse.

La seule partie invariante dans ce schéma reste la boucle de déchiffrement. Les logiciels antivirus utilisent alors cette boucle pour tenter de reconnaitre le programme malveillant.

Un virus oligomorphe est un virus dont le contenu est chiffré systématiquement avec une clé différente et qui contient plusieurs boucles de déchiffrement possibles ; ainsi, chaque version du virus est différente de la précédente.

Un virus polymorphe est un virus oligomorphe qui possède un spectre indénombrable de boucles de déchiffrements possibles. Il est dans ce cas impossible pour un antivirus d'en extraire une signature connue.

Packer Un packer permet la compression de la charge malicieuse à l'aide d'un algorithme particulier au packer. A moins de posséder cet algorithme, il est impossible de dépacker l'exécutable et de l'analyser ; les packers sont maintenant livrés avec des capacités polymorphiques pour à chaque fois rajouter de la complexité dans la détection de la charge malicieuse.

Enfin, la taille de la liste de signatures devient tellement colossale que l'entreprise d'antivirus est contrainte de faire des choix sur les signatures à laisser dans la base ; l'argument souvent proposé consiste à éliminer les signatures des virus les plus vieux et les moins susceptibles de refaire surface. Cependant, ce choix permet à ces vieux virus de passer de nouveaux entre les failles du filet (*sic*).

5.1.6 Fonctionnement et limites de la détection comportementale

Une seconde méthode utilisée (de manière bien moins importante) consiste à faire de l'analyse comportementale de binaires. L'idée est d'exécuter le programme dans un environnement restreint et protégé afin d'étudier les différents appels systèmes et tentatives de connexion sur des serveurs tiers pour apprécier le caractère dangereux d'une application.

Si cette méthode permet de s'affranchir des limites de la reconnaissance par signatures que nous venons d'aborder, elle a également un certain nombre de limites.

La première de ces limites consiste à définir ce qu'est un comportement malveillant, dans la mesure où, pour un système, une telle définition est trop subjective pour être objectivée. Dans certains contextes, un appel système pourra être légitime, alors que dans d'autres, il sera signe d'une tentative de compromission. Ce paradoxe conduit inéluctablement à une zone dans laquelle le programme ne sait pas juger si le programme est réellement malicieux. Le curseur sera alors positionné de manière à trouver un optimum entre fonctionnalité et sécurité. En effet, l'utilisateur géné par les alertes intempestives d'un logiciel antivirus trop sensible aura tendance à se détacher de son jugement.

Par ailleurs, les virus peuvent tester l'environnement dans lequel ils sont en train de s'exécuter ; lorsqu'ils détectent qu'ils sont dans un environnement de type bac à sable, ils avortent avant d'activer la charge malicieuse ; ils sont donc jugés valides par le logiciel antivirus qui permet leur exécution sur la machine.

D'autres méthodes consistent encore à activer la charge virale de manière aléatoire de telle sorte que lorsque l'antivirus vérifie le programme il y a une probabilité suffisante pour qu'il ne trouve pas la charge malicieuse. Dès lors, si l'antivirus utilise des méthodes d'optimisation de performance sur les programmes qu'il a déjà testé, la charge malicieuse pourra être activée lors d'une exécution future alors que l'exécution sera jugée conforme aux règles de sécurité.

5.1.7 Vulnérabilté dans l'AV

Enfin, les antivirus sont des programmes informatiques comme les autres, et dans ce sens ils comportent également des vulnérabilités[135]. Par ailleurs, leur rôle particulier dans le fonctionnement d'un système leur impose d'être exécutés avec des permissions très élevées les transformant en une cible de choix pour les attaquants.

Dès lors, et dans la mesure où un antivirus est appelé à chaque exécution d'un nouveau programme, des programmes malveillants tentent de tirer profits des vulnérabilités du programme antivirus afin de gagner un accès privilégié sur la machine[3].

5.1.8 L'utilisation de l'antivirus reste un MUST

Malgré toutes les limites que nous venons d'étudier, un antivirus reste indispensable pour prévenir certains types d'attaque de masse et ne pas en utiliser serait une erreur grossière. Cependant, l'antivirus de Microsoft *Microsoft Security Essentials* disponible en téléchargement gratuitement reste dans la plupart des contextes la solution à privilégier [13].

Règle 8 : Un antivirus, bien qu'indispensable n'est pas une solution miracle aux enjeux de sécurité informatique ; sa présence ne doit en aucun cas justifier des comportements risqués.

13. Ce type de solutions sera néanmoins à éviter pour certaines PME sensibles qui craignent un espionage aggressif de la part de la firme ou des Etats Unis

5.2 Le cloud computing

Il est souvent légitimement argué que le cloud computing peut être une solution intéressante aux enjeux de cybercriminalité dans la mesure où la sécurité du système est gérée par une entreprise spécialisée, censée maitriser ces problématiques bien mieux qu'une PME dont le coeur de métier est souvent bien loin de ce type de considérations.

5.2.1 Définition du cloud computing

Le cloud computing, défini par le NIST comme *" a pay-per-use model for enabling available, convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"*[123], permet pour un client de s'affranchir complètement des questions relatives à la résiliences ou à la sécurité de base d'un système, les déléguant de fait au prestataire de service. Ainsi, le client tire un profit complet des toutes dernières technologies, d'une architecture résiliente et sauvegardée régulièrement avec des plans de reprise d'activité calibrés par rapport à ses besoins.

Cependant, il y a quelques pièges dans lesquels il faut prendre soin de ne pas tomber.

5.2.2 La délocalisation des données

La délocalisation de ses données peut impliquer la perte de souveraineté sur ses données ; par exemple, la loi du *patriot act*[23] oblige les entreprises dont le siège est situé aux Etats Unis ainsi que leurs filiales situées en dehors des Etats-Unis à remonter des données vers les autorités des Etats Unis. Dès lors, dans un contexte professionnel où les notions de propriété intellectuelle sont importantes, on préfèrera utiliser un prestataire de service français[125] dont les centres de données utilisés sont exclusivement en France. On se prémunit ainsi de certains accès légaux de la part de gouvernements ou sociétés étrangères sur les données confidentielles. On évitera alors particulièrement les solutions proposées par des services américains comme Micosoft[142], Dropbox, Google ou Amazon pourtant souvent cités comme des solutions intuitives et très fonctionnelles.

5.2.3 La relation de confiance

Par ailleurs la relation de confiance avec le prestataire est primordiale. "Parce que, lorsqu'une donnée circule dans le nuage, des centaines de techniciens y ont accès. Par le jeu de la sous-traitance, plus de la moitié d'entre eux ne sont pas en France", assure Hervé Schauer, membre du Club de la sécurité de l'information français (Clusif) et expert en sécurité des systèmes d'information[124]. "Si l'une de ces personnes est corrompue, il n'y a plus de confidentialité dans le cloud." Il est donc primordial que le prestataire ait mis en place une architecture techniquement cloisonnée qui permette de gérer les permissions d'accès de manière aussi granuleuse que possible.

Il est de plus indispensable que les services du prestataire incluent des items liés à la sécurité, comme la présence d'un antivirus à jour et à l'état de l'art, une protection de type pare-feux, la sauvegarde régulière des données, la mise en place d'un PRA et d'un PCA, la mise en place de système à l'état de l'art en sécurité et l'application d'une politique de mise à jour des patchs de sécurité très régulière, ainsi qu'un contrôle très granuleux des accès et la possibilité de chiffrer au minimum les informations confidentielles et au mieux l'intégralité des disques.

5.2.4 Une confiance dans la certification ANSSI

Il est fondamental de bien comprendre qu'il s'agit de délocaliser son système d'information ainsi que la totalité des données opérationnelles ; pour ces raisons il est primordial de se poser la question du risque pour l'entreprise de stocker ses données chez un prestataire tiers, compte tenu des risques exposés plus haut. Pour des questions de confiance, on préfèrera autant que faire se peut faire le choix de prestataires labélisés de confiance par l'ANSSI, ou certifiés par des pretataires labellisés ANSSI.

La question de la confiance, fondamentale dans le choix d'un prestataire sera évoquée plus largement par la suite.

Par ailleurs, même si le cloud computing peut permettre une réduction conséquente des risques liés aux systèmes opérationnels, il ne protège en rien les applications ou les utilisateurs finals.

5.2.5 La sécurité des utilisateurs finals

Le cloud computing, s'il permet de virtualiser les systèmes opérationnels, ne concerne pas les stations de travail des utilisateurs finals. Dès lors, une mauvaise protection de la station de travail ou une conduite à risque de son utilisateur permettra un accès privilégié depuis cette station compromise vers les centres de données délocalisés dans le cloud. Ainsi, le cyber attaquant pourra afin d'attaquer un ensemble mieux sécurisé passer par le maillon faible et parvenir à ses fins en une bande.

5.2.6 La sécurité des applications web

Une application web est une application manipulable au moyen d'un navigateur web (par exemple Firefox, Chrome, Safari,...). Les applications web correspondent au coeur des applications métiers. Elles permettent une intéraction avec un utilisateur et interfacent une grande partie des opérations métier.

D'un point de vue informatique, les applications web affichent, en fonction des requêtes des utilisateurs, des contenus générés dynamiquement par le *backend* de l'application ou peuvent parfois les modifier.

La plupart du temps le cylcle d'affichage se déroule comme suit ; le serveur HTTP reçoit la requête et la transfère au serveur applicatif ; ce dernier lance le script correspondant et fait des appels à la base de données afin de générer le code source de la page web contenant les informations demandées par le client. Cette page au format HTML est ensuite renvoyée au serveur web qui la renvoie au client. Le navigateur web interprète le code HTML renvoyé par le serveur et l'affiche sur l'écran.

Cependant, il est possible que l'utilisateur passe au serveur des requêtes avec des paramètres forgés de manière à détourner le comportement normal de l'application[85]. Il peut par exemple être possible sous certaines conditions de récupérer par ce moyen l'intégralité de la base de données de l'application [85]. Il peut également être possible par ce biais d'injecter dans les bases de données un code malveillant de telle sorte qu'à chaque requête le serveur de base de données, l'application et enfin le serveur web renvoient un contenu HTML modifié et contenant des parcelles malicieuses[85].

Ce genre d'attaque, dûe à une mauvaise validation des paramètres passés par les utilisateurs, est possible quelque soit le type d'infrastructures sous jacentes. Le cloud computing ne permet dès lors *a priori* pas de prévenir ce genre de vulnérabilités [14].

Par ailleurs, un mauvais contrôle d'accès des informations des ressources peut engendrer la mise à disposition d'une partie parfois sensible des données directement pour des utilisateurs ne disposant pas de ces permissions, voire les indexer sur google[97][104].

Enfin, il est possible sous certaines conditions d'exploiter de telles failles pour prendre entièrement la main sur le système cible ce qui peut conduire, selon les cas aux conséquences évoquées dans les parties précédentes (défacement, mise à profit d'une pub de type pay per click, utilisation des ressources du serveur et hébergement d'activités illégales...)

Dans tous ces cas, c'est la sécurité de l'application web en tant que telle qui est mise à mal, pas la sécurité du système, la seule protégée *a priori* par le prestataire de cloud.

Règle 9 : Le cloud computing n'est pas une solution miracle aux enjeux de sécurité et ne réduit qu'une partie de la surface d'attaque ; les applications ainsi que les clients finals restent des cibles tout autant exposées. Par ailleurs, la délocalisation de son informatique ne peut être envisagée qu'auprès de prestataires de confiance.

Recommandation 12 : La construction d'applications web en interne comme en externe doit être suivie par des prestataires de confiance et la sécurité de ces applications doit être auditée de manière régulière.

14. certains services à la demande permettent d'ajouter des parefeux applicatifs dont l'objectif est de détecter, sous certaines conditions, les attaques correspondantes

Nous avons démontré dans les parties précédentes qu'il n'existe à ce jour aucune solution technique unique qui puisse intégrer parfaitement les contraintes de sécurité de l'ensemble des petites et moyennes entreprises. Dès lors il est primordial d'inciter au travers de leviers économiques les entreprises à adopter des comportements plus responsables. Cette étude a identifié deux leviers économiques fondamentaux : la Banque de France dans son rôle d'Organisme Evaluateur de Crédits et les assurances dans leur rôle de soutien à la continuité d'activité suite à la survenue d'un incident. Ces deux leviers devraient participer à l'emmergence d'une atmosphère plus propice à la prise de conscience des enjeux de cybersécurité qui devrait entrainer dans son sillage une grande partie des entreprises et par la même la hausse du niveau général de la cybersécurité.

6 La cotation Banque de France

6.1 Le principe de la création monétaire

6.1.1 Création monétaire par la banque commerciale

Lorsqu'elle souhaite financer un projet d'investissement, ou que sa trésorerie s'avère insuffisante, une entreprise prend naturellement l'attache de sa banque commerciale, afin de lui demander l'octroi d'un crédit ou d'une ligne de trésorerie. Si la banque accepte, elle inscrit le droit de tirage au passif de son bilan, en échange d'un titre de créance porté à son actif. Ce processus contribue à l'action de création monétaire par les banques commerciales.

A l'opposé la « destruction » monétaire intervient lorsque l'emprunt ou de la ligne de trésorerie sont remboursés : les éléments inscrits au passif et à l'actif s'annulent, et sont retirés du bilan de la banque commerciale.

6.1.2 La création monétaire par la banque centrale

Les régulateurs bancaires contraignent les banques, dans un souci de stabilité financière, à respecter un niveau minimum de capitaux propres par rapport aux crédits accordés. De fait, cela revient à limiter le montant des crédits distribués aux entreprises, en sélectionnant ceux qui présentent le moins de risques.

Par ailleurs, les constants et importants besoins en liquidité de la part des banques commerciales leur imposent de se refinancer à leur tour et de manière très régulière soit sur les marchés, soit auprès d'une banque centrale, l'Eurosystème pour les banques commerciales européennes.

Lorsqu'elle désire se refinancer, la banque commerciale suit un mécanisme similaire et met certains types d'actifs à disposition de sa banque centrale en échange de liquidité. Ce mécanisme se nomme la prise en pension. Les prêts sont effectués sur des durées très courtes (quelques jours) et aux taux BCE. La monnaie ainsi créée disparaît dès son retour à la Banque Centrale, à la fin de la prise en pension.

6.2 Le principe de la cotation

6.2.1 La nécessité d'une cotation indépendante

Afin d'assurer la stabilité du système et pour limiter le risque de crédit, la Banque centrale n'accepte que des titres de très grande qualité, c'est à dire dont la probabilité de remboursement est la plus importante possible. C'est par exemple le cas pour les bons du trésor ou des titres de créances privées de qualité.

Il est donc fondamental d'avoir des organismes externes et neutres d'évaluation du crédit dont l'objectif est de noter les créances des entreprises privées, c'est à dire d'évaluer "la capacité d'un émetteur ou d'une émission de titres à faire face en temps et en heure aux engagements financiers à terme (paiement d'intérêts, de dividendes préférentiels, ou remboursement du principal)" [45]

Lorsqu'elles accordent un crédit, les banques commerciales sont extrêmement sensibles à cette notation dans la mesure où la qualité des titres de créances qu'elle acquièrent leur permettent, ou non, de se refinancer auprès des banques centrales. Par ailleurs, afin de diminuer son risque de crédit, la banque commerciale a pour obligation de limiter à une certaine proportion les prêts *risqués*, c'est à dire les prêts offerts à des entreprises dont la cotation est faible.

6.2.2 Les organismes de cotation

En France, six établissement ont été reconnus en tant qu'OEEC par la commission bancaire[13] :

- Banque de France
- Dominion Bond Rating Services
- Fitch Ratings
- Japan Credit Rating Agency
- Moody's Investors Services
- Standard & Poor's Ratings services

6.3 La cotation Banque de France

La Banque de France a été inscrite sur la liste des OEEC par décision de la Commission bancaire le 19 juin 2007[45]

6.3.1 Un rôle pédagogique

Parmi les organismes d'évaluation externe de crédit, la Banque de France côte tous les ans pres de 300 000 entreprises. Elle présente la particularité d'être l'interlocuteur de choix lorsqu'il s'agit de la cotation des PME dans la mesure où elle évalue au moins une fois par an toutes les entreprises dont le chiffre d'affaires est supérieur à 750 000 euros. Sa cotation est une "appréciation sur la capacité de l'entreprise à faire face à ses engagements financiers à un horizon trois ans"[45].

En outre, la Banque de France se deplace auprès de 50 000 entreprises tous les ans afin de faire une analyse plus approfondie de leur situation. Cette rencontre a également un rôle pédagogique car les représentants Banque de France partagent leur experience du risque et insistent sur l'importance de sa prise en compte dans un spectre aussi large que possible. Cette opération de sensibilisation aux risques permet alors aux chefs d'entreprises de mieux prévenir la survenue d'incidents innattendus et de participer à la construction d'un cadre global aussi favorable que possible à la pérennité de leur activité.

6.3.2 La diversité des risques appréciés

Lors de son analyse, la Banque de France intègre une grande diversite de risques au travers de la prise en compte d'éléments aussi bien qualitatifs que quantitatifs. Cette palette de risques est ensuite projetée sur l'axe financier afin d'en apprécier les impacts sur le bilan financier et l'activité de l'entreprise à horizon 3 ans. De cette projection résulte la cotation définitive qui sera attribuée à l'entreprise.

6.3.3 Intégration du risque cyber dans la cotation

Comme étudié précédemment, le risque cyber peut avoir des conséquences notoires pour l'entreprise et l'empêcher d'honorer certains engagements financiers. Plusieurs éléments peuvent se combiner à cet effet, que ce soit le coût de remise en marche de l'outil de production ou le coût afférent à la vente de produits non conformes, voire celui résultant de la dégradation de la réputation de l'entreprise ou de l'image de marque associée à ses produits. Le vol de propriété intellectuelle peut également conduire à la perte de sources de revenus sur le long terme ou encore le paiement d'une rançon est perçu comme une *perte sèche*, dont résultera à son tour, une difficulté à honorer ses engagements.

Notons par ailleurs que le risque opérationnel est intégré dans la démarche d'évaluation des risques par le secteur bancaire depuis les accords prudentiels dits de Bâle 2. Ce risque est en particulier évalué dans ses aspects liés à la cybersécurité. Cependant cette approche, obligatoire au regard des processus internes au secteur bancaire, n'a pour le moment point été déclinée par la Banque de France dans le cadre de sa cartographie actuelle des risques appliquée aux entreprises qu'elle évalue.

Nous proposons donc la prise en compte du risque cyber dans la matrice de cotation de la Banque de France.

6.4 Mise en pratique

6.4.1 Création d'un kit d'autoévaluation

La fonction d'organisme évaluateur confiée à la Banque de France, consiste à apprécier l'impact de différents risques sur le bilan financier de l'entreprise. Toutefois ces risques peuvent s'avérer de différentes natures, cette nature même échappant souvent au domaine de compétences de la Banque de France.

La cybersécurité n'échappe pas à cette analyse, la Banque de France n'étant pas un organisme reconnu pour son expertise dans le domaine. Il n'est donc pas question que la Banque de France devienne un nouvel étalissement de normes dans le domaine de la sécurité ou une nouvelle entité de contrôle des systèmes d'information. L'idée serait donc qu'elle travaille de concert avec des institutions comme l'ANSSI, la DGSI ou encore avec la D2IE afin de mettre au point une sorte de kit évaluant le niveau global de sécurité d'une société au travers d'un questionnaire simple. Le format pourrait être assez proche de l'outil DIESE[26] mis à disposition des entreprises en 2014 par la D2IE ; ce kit est composé de 84 questions englobant divers aspects liés à l'exposition d'une part et à la sensibilité de l'entreprise en matière de sécurité des systèmes d'information d'autre part.

La note finale résultante de ce questionnaire serait alors intégrée à la cotation de la banque de France, pondérée par un coefficient de risque cyber calculé par la Banque de France.

Enfin, l'utilisation d'un outil comme DIESE permettrait d'évaluer les points faibles dans la protection de l'entreprise permettant à cette dernière de prendre conscience de sa vulnérabilité et donc de se renforcer aux endroits où sa protection est insuffisante.

6.4.2 Pousuivre le rôle pédagogique

Par ailleurs, dans son rôle d'éducation, la Banque de France pourrait alors inclure ce risque dans la pallette des risques présentés et participer à la construction d'un climat plus propice à la prise en compte des enjeux de cybersécurité.

Il lui serait par exemple possible de délivrer une plaquette reprenant les règles d'hygiène comportementales présentées dans ce rapport.

Une telle mesure incitative permettrait donc aux entreprises désireuses de bénéficier de conditions d'emprunt préférentielles auprès de leur banque commerciale d'inclure des process peu coûteux qui amélioreraient déjà de manière conséquente le niveau de sécurité de l'entreprise.

7 Renforcement des mécanismes assurantiels

La possibilité d'obtention de prêts bancaires à un taux préférentiel en contrepartie de l'intégration de mesures permettant de prévenir le risque cyber, apparaît de nature à modifier significativement l'approche du sujet par les PME. Toutefois, au delà de cette prise de conscience et de la mise en place de mesures qui en découle, les auteurs du présent mémoire sont convaincus de l'intérêt d'une couverture des risques résiduels à l'aide d'un second mécanisme économique : le dispositif assurantiel.

7.1 Business model d'une assurance

L'aversion au risque d'une part et la recherche d'une possibilité de continuité d'activité (ou de reprise rapide d'activité) en cas de survenue d'un incident, tout en diminuant les conséquences financières sur le bilan, d'autre part, constituent deux des caractéristiques intrinsèques des investisseurs auxquelles ne sauraient se soustraire les entreprises. Pour répondre à ces inquiétudes, il est possible de transformer une logique de coûts variables non prédictibles et potentiellement exorbitants (le paiement lors de la survenue de l'incident de l'intégralité des coûts afférents) en une logique de coûts fixes. Il s'agit de la base du mécanisme assurantiel.

Pour une entreprise, deux mécanismes assurantiels spécifiques peuvent coexister[57] :
- la prévention à titre individuel,
- le transfert des risques vers un tiers (réassurance).

7.1.1 L'autoassurance

Sur le plan individuel, la prévention –ou l'autoassurance– est souvent utilisée et intervient généralement avec la notion de diversification du risque ; ce mécanisme peut être résumé par la maxime *"ne pas mettre tous les oeufs dans le même panier"*.

Ainsi, la diversification des solutions techniques, même si elle rajoute des coûts d'interconnexion ainsi qu'une certaine complexité, permet lors de la potentielle découverte d'une vulnérabilité critique sur un logiciel précis de poursuivre son activité en basculant le traitement de la dite activité sur d'autres logiciels non affectés, le temps que la faille soit corrigée.

7.1.2 Le transfert vers un tiers

Il est également possible pour une société de transférer une partie de son risque vers une compagnie d'assurance ; cette dernière utilise alors le principe de mutualisation des risques.

La mutualisation des risques a pour vocation d'éviter la ruine ou la misère d'une entreprise isolée ou d'un individuel lors de la survenue d'un accident dont la potentialité touche un grand nombre.

Dans ce schéma, l'aléa menace un grand nombre d'entreprises. L'agrégation des risques indépendants à l'intérieur d'une structure assurantielle commune se fonde sur l'utilisation de la loi des grands nombres qui exprime le fait que les caractéristiques d'un échantillon aléatoire se rapprochent d'autant plus des caractéristiques statistiques de la population que la taille de l'échantillon augmente [144]. Il est donc possible au moyen de modèles mathématiques statistiques de prévoir le nombre d'occurences d'un évènement probable ainsi que les coûts qui lui seront associés.

Le risque devient alors globalement éliminable puisque prédictible par la société d'assurance : l'aléa n'affecte plus la masse totale des ressources, mais seulement la répartition de ces ressources entre les agents. L'idée générale est alors de répartir la charge entre un grand nombre d'acteurs (les assurés) afin que chacun de ceux-ci ne supportent virtuellement qu'une très faible part du risque initial.

La société d'assurance fonctionne sur une asymétrie totale du rapport entre assuré et assureur : le premier s'acquitte en premier lieu d'une prime d'assurance constituant la contrepartie d'une prise en charge complète [15] par la compagnie des conséquences financières en cas de survenue d'un incident. L'assuré n'est, la plupart du temps, tenu à aucune autre forme de solidarité *ex post*.

Le modèle économique est ainsi inversé : l'assurance perçoit un profit avant la potentielle réalisation du service associé, mais doit en contrepartie comptabiliser des provisions techniques à son bilan correspondant à ses engagements.

Le modèle assurantiel se fonde sur un excédent en fonds de roulement, que la société d'assurance investira auprès d'autres acteurs demandeurs de liquidités afin d'en tirer une plus-value. A noter cependant que l'existence d'une forte concurrence sur certains secteurs de la branche « Non Vie » (Assurance Habitation, Automobile,..) amène à un bénéfice net contrasté en fonction du risque couvert.

L'existence d'une prime de risque ouvre ici la possibilité de transferts mutuellement avantageux dès l'instant où l'une des parties (l'assurance) dispose d'une aversion au risque plus faible que l'autre.

Le danger d'un tel mécanisme cependant provient du fait qu'une telle couverture du risque peut décourager la prévention et favoriser la prise de risque, augmentant donc le risque global. Il est alors fondamental pour l'assureur de définir un cadre précis dans lequel le mécanisme assurantiel est activable. Ce cadre est alors précisé dans le contrat d'assurance

Dans notre étude, les sociétés s'assurant contre le risque cyber devrait par exemple fournir la preuve que l'infraction n'est pas dûe à une négligence caractérisée.

15. une franchise peut être exigée

Ce point constitue cependant un point délicat du modèle dans la mesure où contrairement à un cambrioloage pour lequel les verrous d'une porte sont soit absents, soit cassés par le cambrioleur (il est donc possible de déterminer s'il y a eu négligence de la part de l'assuré), dans le cas d'une intrusion informatique, la personne malveillante s'est forcément infiltrée via une vulnérabilité (c'est à dire schématiquement une porte mal fermée), la plupart du temps engendrée par un défaut de conception ou de développement.

Que ce soit une erreur humaine lors du développement ou du déploiement d'un logiciel, une erreur humaine lors de l'ouverture d'un email contenant une pièce jointe malveillante, ou la non mise à jour de certains composants souffrant de vulnérabilités (se pose alors la question de la possibilité de mise à jour en production et en un temps assez court des composants sans affecter de manière sûre la chaine de production[8][106]), il est alors important de fixer la limite au delà de laquelle la négligence sera qualifiée.

Enfin, il parait fondamental de se pencher sur le fait que, contrairement aux verrous, la plupart des applications et des systèmes d'exploitation sont périssables et qu'ils ne sont maintenus que pour un lapse de temps prédéfini. Dès lors, pour ne prendre qu'un exemple, le système d'exploitation de Microsoft, Windows XP, est officiellement arrivé en fin de vie le 8 avril 2014[6]. Malgré le fait que son support ait été suspendu, et que par conséquent toutes les nouvelles vulnérabilités trouvées ne pourront plus être corrigées, sa part de marché reste au dessus de 35% au Etats-Unis[82]. En France, 40% des postes informatiques des clients de Capgemini-Sogeti tourneraient sous Windows XP ; cette proportion grimperait à 50% chez Steria, 60% de la clientèle de grands-comptes chez Econocom-Osiatis, et jusqu'à 70% chez les clients de Bull[66]. Se pose alors la question de l'assurabilité d'entreprises utilisant de tels systèmes mais également des coûts associés aux migrations nécessaires.

7.2 Le développement massif du secteur de la cyber-assurance

7.2.1 Un marché essentiellement etats-unien

Dans toute la suite, les assurances cyber, ou cyber assurances désignent indifféremment les assurances dédiées à la couverture des risques liés à la cybercriminalité. Aux Etats Unis, ce segment du marché assurantiel a connu une croissance spectaculaire sur les dernières années pour être souscrit début 2014 par plus de 30% des entreprises [126] pour un montant de primes estimées à 1,3 milliards de dollars[34].

Cette tendance semble par ailleurs se généraliser : une étude menée par le groupe Allianz auprès de 400 assureurs dans 30 pays atteste que les risques liés à l'informatique ont bondi du 15ème au 8ème rang des préoccupations des chefs d'entreprise. Le marché, aujourd'hui dominé par les assureurs AIG, Zurich et quelques syndicats des Lloyd's dont Beazley et Hiscox, demeure à la recherche d'un modèle économique stable ; cette incertitude permet à des géants de la profession tels que Allianz et Axa de se faire une place sur ce segment en proposant une nouvelle offre différenciée en 2013[139].

7.2.2 La responsabilité des données

La cyber-assurance est née sur le continent américain il y tout juste une décennie ; sa croissance y a été stimulée non seulement par une augmentation de la cybercriminalité, mais aussi et avant tout par une réglementation américaine qui accroit considérablement l'aversion des entreprises aux cyber risques.

En effet, la plupart des Etats états-uniens exigent que les entreprises informent leurs clients en cas de suspicion de perte de données personnelles. les entreprises informent leurs clients en cas de violation ou de perte des données personnelles les concernant. De ce fait, la responsabilité des entreprises peut être recherchée au travers de recours collectifs, les *class actions* les contraignant à de fortes amendes en cas de responsabilité avérée.

Ces amendes juridiques viennent encore augmenter les conséquences financières déjà très lourdes des cyber attaques (qui cumule l'arrêt potentiel de la production, l'indemnisation des retards de production, la déterioration de la notoriété, ...)[107][127] et les poussant alors à déporter les risques cyber vers des sociétés d'assurance adaptées.

En France, le paradigme est différent ; seuls les fournisseurs de services de communications électroniques ont l'obligation de notifier les violations de données personnelles aux autorités nationales compétentes et, dans certains cas, aux personnes concernées. Cette obligation a été transposée en droit français à l'article 34 bis de la loi " Informatique et Libertés "[32].

L'adoption de la Loi de Programmation Militaire[91] (LPM) de décembre 2013 a de plus instauré pour chaque Opérateur d'Importance Vitale [16] l'obligation de déclarer à l'ANSSI les intrusions constatées dans les systèmes d'information. Ces notifications ne concernent cependant pas les clients.

7.2.3 Les réglementations catalysent le développement du marché de l'assurance

La réglementation devrait néanmoins évoluer assez rapidement en France sur ce point, l'Union Européenne marquant une volonté forte pour la notification publique de toutes les compromissions d'un système d'information[112], ce qui devrait constituer un cadre propice au développement du marché assurantiel.

Une autre différence majeure provient du fait qu'en France, certains actes ne peuvent pas être légalement indemnisés ; c'est par exemple le cas du paiement de rançons. Un tel cas de figure impose donc aux assurés de ne pas répondre aux demandes de rançons lors de la compromission de leurs systèmes d'information, et donc de s'exposer à l'effacement pur et simple de leurs données s'ils souhaitent être indemnisés par leur assureur Se pose alors la question des délais de remboursements et des protocoles d'aide mis en place par les assureurs afin de respecter le plan de reprise d'activité.

16. Définition ANSSI, dont la liste est classifiée

L'assureur prendrait alors en charge financièrement toute l'investigation, la décontamination, la récupération et la reconstitution des données afin que la société soit en mesure de poursuivre ou de reprendre son activité dans les plus brefs délais. Pour ce faire, il pourra développer des accords partenariaux avec des sociétés spécialisées à qui il déléguerait les plans de reprise et de continuité d'activité.

La loi sur la consommation du 17 mars 2014 (dite loi Hamon)[89] a par ailleurs introduit la possibilité de *class actions* à la française, en ouvrant ce droit aux associations de consommateurs agréées par l'Etat. Cette perspective, saluée comme une avancée significative face au retard accumulé dans cette voie par rapport à nos partenaires européens, permettra donc le recours collectif à l'encontre de structures ou entreprises à l'origine de la divulgation de données personnelles. La France pourra ainsi prochainement présenter un contexte relativement similaire à celui existant au Etats Unis, et de ce fait favoriser l'éclosion et le développement du marché de la cyber assurance.

7.3 Mise en place d'une offre dédiée

7.3.1 Un modèle existant pour les grands groupes

Le marché de l'assurance cyber est déjà une réalité pour les grandes entreprises qui craignent de venir grossir les 445 milliards de dollars de pertes subies par les entreprises[107].

Les prestataires reconnus et dont le coeur de métier s'oriente autour de problématiques connexes à la cybersécurité se sont ainsi adossés aux compagnies d'assurance afin de proposer des offres liées ; on compte alors de nombreux binomes comme Beazley et Logica, Marsh et Sogeti ou encore AXA Matrix et Airbus Defense and Space ou Allianz et Thales.

La partie du binome dont le coeur de métier est orienté sur des aspects technologiques établit au moyen d'une étude approfondie le niveau de risque global et le réduit au maximum par des solutions techniques adaptées ainsi qu'au travers de la modification de certains processus métier. Le risque résiduel est alors déporté dans un second temps vers la partie assurance du binôme.

7.3.2 Un embryon de modèle pour les PME

Cependant, si de telles structures semblent relativement bien fonctionner pour des entreprises de taille importante, le coût qu'elles imposent ne semble pas adapté aux petites et moyennes entreprises pour lesquelles la simple partie d'étude et d'analyse de la sécurité du système d'information est déjà souvent non supportable.

En conséquence, certaines sociétés d'assurance, comme AXA réfléchissent un modèle alternatif, dédié aux PME, et qui se déclinerait de manière assez similaire à celui décrit dans la partie précédente (voir 6.4, P63).

Les compagnies d'assurance pourraient alors proposer une sorte de questionnaire corédigé avec leurs partenaires et qui permettrait d'apprécier le niveau global d'exposition de la société assurée. Il est bien évident que la police d'assurance devra être fonction de l'exposition globale de l'entreprise : de son niveau intrinsèque de sécurité, mais aussi de l'exposition de la filière de son coeur de métier, de la répartition géographique de ses systèmes et outils de production, etc.

La compagnie d'assurance pourrait ainsi déterminer, en fonction du niveau de risque, une prime d'assurance correspondante ; l'entreprise chercherait donc son optimum économique en mettant en place des mesures simples visant à réduire son risque et de façon à diminuer le montant de sa prime d'assurance.

Ce modèle est par exemple déjà utilisé lors de l'assurance contre les cambriolages. L'industrie des blindages offre des produits certifiés qui sont classifiés en utilisant un nombre d'étoiles différent selon la sécurité offerte par le blindage, c'est à dire le temps de résistance à l'effraction réalisée en laboratoire. Lors de la souscription à une assurance, les montants de la prime d'assurance sont alors fonction, entre autres, de la qualité de blindage mise en place. De même dans ce cas, la prime d'assurance devra être fonction de la qualité des systèmes mis en place afin de prévenir les intrusions.

L'évaluation de l'entreprise par l'assurance pourrait par exemple se fonder sur divers éléments économiques (chiffre d'affaires de l'entreprise, exposition de l'activité au niveau international, exposition des clients, ...), et sur un questionnaire hérité des critères communs ou dérivé des mesures d'hygiène de l'ANSSI. A ce titre, la Délégation Interministérielle à l'Intelligence Economique (D2IE) propose désormais gratuitement l'outil DIESE, qui pourrait servir de canevas d'analyse.

Ainsi, afin de ne pas avoir à supporter des coûts de police d'assurance trop conséquents, l'entreprise ferait alors probablement son calcul de coûts / bénéfices et pourrait ainsi être encline à renforcer son niveau de sécurité par des mesures simples et peu onéreuses, assurant ensuite le risque résiduel à moindre coût.

Par ailleurs, la valeur des actifs étant de fait moins importante pour une PME que pour un grand groupe, une diminution des montants remboursés permettrait certainement de diminuer les montants des primes d'assurance.

7.3.3 Un modèle qui se cherche

En outre faute d'obligation légale de signalement aux autorités judiciaires, les préjudices demeurent aujourd'hui assez méconnus tant dans leur nombre, que dans leurs évaluations financières ce qui complique l'établissement d'un modèle pertinent. Le principe même de l'évaluation financière d'une donnée peut d'ailleurs nourrir bien des débats ; comment en effet évaluer le préjudice subi lors d'un vol de brevet ou l'impact financier d'une cyber-attaque sur la réputation et l'image d'une PME ?

Les assurances qui disposent d'un périmètre d'intervention global, peuvent toutefois tirer parti de leur expérience sur d'autres marchés plus matures, pour profiler et proposer de premières offres de couverture. Cette entrée en la matière permettra d'amorcer le mouvement, en incluant l'obligation pour les assurés de déposer plainte s'ils veulent se voir indemnisés.

7.3.4 Constitution d'un cercle vertueux

Un tel processus permettrait ainsi à l'état de posséder des données plus précises quant au développement de la cybercriminalité et son coût réel pour l'économie.

L'expérience du marché de l'assurance « vol » relatif aux téléphones portables est une parfaite illustration de ce mécanisme : ce n'est qu'après l'institution du dépôt de plainte obligatoire par les assureurs que des statistiques complètes ont pu être établies, et avec elles, l'adaptation des modèles assurantiels.

Du point de vue des banques et assurances la cybersécurité constitue un nouveau marché et non un coût[139]. A l'image d'une industrie automobile qui a vu les lobbies insister auprès des constructeurs pour un niveau de sécurité renforcée, on peut s'attendre à ce que les acteurs du financement encouragent fortement l'émergence d'une offre de cybersécurité afin d'augmenter les profits liés aux mécanismes d'assurance.

8 Développement d'un modèle basé sur une offre de service

Les mesures détaillées dans les parties précédentes proposent une démarche incitative pour l'élaboration progressive d'un climat de responsabilisation et de prudence vis-à-vis des enjeux liés à la cybersécurité. Cependant, il est primordial qu'une offre de produits dédiés aux PME ou aux structures similaires soit mise à disposition de ces dernières afin que les démarches de sécurisation puissent s'intégrer dans un référentiel commun, partagé et de confiance. Ces offres pourraient alors servir à la fois la commande publique dont la structure, comme analysé avant, peut être voisine de celle des PME, et les entreprises privées.

8.1 Les efforts de l'Etat pour soutenir l'industrie

Volontaire pour soutenir une industrie dont il a bien compris qu'au delà du levier économique sans précédent qu'elle constitue, elle lui permettra également de garantir la protection de la propriété intellectuelle de ses entreprises et donc la pérennité de l'industrie française en plus de garantir sa propre souveraineté, l'Etat multiplie les actions pour soutenir la filière numérique et les projets visant à la sécuriser. Entre autres actions, 3 pilliers semblent se dégager qui représentent une stratégie dont les résultats sont attendus à court, moyen et long terme.

8.1.1 A court terme, les pôles de compétitivité

"Les pôles de compétitivité sont constitués par le regroupement sur un même territoire d'entreprises, d'établissements d'enseignement supérieur et d'organismes de recherche publics ou privés qui ont vocation à travailler en synergie pour mettre en oeuvre des projets de développement économique pour l'innovation" , d'après la loi n° 2004-1484 du 30 décembre 2004 de finances pour 2005[92]. Dans la pratique il s'agit de 71 clusters, bénéficiant de subventions publiques et de régimes fiscaux particuliers, qui sont regroupés autour de thématiques diverses comme l'aéronautique, l'agriculture, les bioressources, les biotechnologies, l'énergie, les écotechnologies,... Il existe ainsi des pôles de compétitivité centrés sur les thématiques de cybersécurité.

Solutions Communicantes Sécurisées par exemple, est un pôle de compétitivité international situé à Sophia Antipolis, regroupant entre autres 25 grandes entreprises et 186 PME [15] , et dont l'ambition affichée est de devenir un acteur incontournable et reconnu dans le domaine des Solutions Communicantes Sécurisées en couvrant l'ensemble de la chaîne de valeur des métiers des TIC, du Silicium aux Usages[10]

Transactions électroniques sécurisées, localisé en Normandie, regroupe quant à lui 11 grandes entreprises et 73 PME [18] , autour d'un écosystème innovant pour sécuriser l'ensemble des techniques électroniques, informatiques et télématiques permettant d'effectuer des échanges d'informations[11]

8.1.2 A moyen terme, les Programmes d'Investissement d'Avenir

Dans le prolongement des conclusions de la Commission sur les priorités stratégiques d'investissement et l'emprunt national, la loi de finances rectificative pour 2010 prévoit la mise en oeuvre d'un programme d'investissements d'avenir pour un montant de 35 milliards d'euros. L'objectif du programme est de moderniser et de renforcer la compétitivité française, en favorisant l'investissement et l'innovation dans 5 secteurs prioritaires, générateurs de croissance et d'emplois ; le numérique est identidié comme l'un des secteurs prioritaires.

Ainsi, dans la partie des Programmes d'Investissement d'Avenir structurée autour du coeur de filière numérique[64], l'Etat, au travers de la DGCIS, a lancé des appels à projet, corédigés avec l'ANSSI, afin de favoriser l'emmergence de solutions techniques en adéquation avec les besoins identifiés par les professionnels du secteur.

8.1.3 A long terme, les plans pour la nouvelle France industrielle

Dans sa feuille de route pour la mise en place des 34 plans pour la nouvelle France industrielle[109] , le ministre du redressement productif Arnaud Montebourg a largement inséré la problématique des nouvelles technologies et particulièrement les enjeux liés à la cybersécurité en leur dédiant un plan sous le contrôle de l'ANSSI. Ce plan a pour objectif de développer une offre industrielle française robuste qui puisse s'exporter à l'international et passe ainsi par plusieurs mesures clé tels que :

- Accroitre la demande en solutions de cybersécurité de confiance
- Développer pour les besoins de la France des offres de confiance
- Organiser l'exportation à l'international des produits français
- Renforcer les entreprises nationales et favoriser l'emmergence d'ETI

Il apparait donc que l'Etat met en place une riche palette de plans afin d'accélérer la mise en place à court, moyen et long terme de solutions répondant aux enjeux de la cybersécurité. Cependant, il semblerait que jusqu'à présent, et malgré le besoin de plus en plus exprimé, les petites et moyennes entreprises ne parviennent pas à trouver des outils ou des solutions qui permettent de répondre à leurs situations avec des coûts acceptables.

Ce rapport s'interroge donc sur la possibilité de changer le paradigme du développement de ces solutions logicielles en se retournant vers un modèle *open source*.

8.2 Le modèle open source

8.2.1 L'open source, à la base du fonctionnement d'internet

Le modèle *open source*[17] est un modèle de développement dans lequel les codes sources des logiciels sont mis à disposition d'une communauté afin que

17. Malgré les différences, ce rapport considère comme synonymes les modèles libres et open source et se permet cet abus de langage pour des questions de lisibilité ; le lecteur intéressé par la différence entre ces modèles pourra se retourne vers la lecture de [SOURCE]

celle-ci puisse l'utiliser librement et lui apporter, en cas de nécessité, de nouvelles fonctionnalités qui seront alors intégrées à leur tour et mises à disposition de la communauté. Il s'agit en ce sens d'un modèle d'innovation ouverte qui s'oppose au modèle d'innovation protégée par les licenses dans lequel une innovation reste propriété du groupe par lequel elle a été produite. Ce modèle pousse alors à une innovation croissante axée plus sur la qualité technique du produit et moins sur une stratégie de rente technologique soutenue par le *marketing* et les équipes commerciales. C'est alors une innovation continue déclinée à la fois sur les procuits et les services associés qui permet à un tel modèle de fonctionner.

Ce modèle est en réalité à la base d'Internet, pour lequel près de 70% des sites actifs sont hébergés par des serveurs *open sources* (principalement Apache et Nginx -cette proportion est encore plus importante pour les serveurs du million de sites le plus actifs) et est omiprésent dans la plupart des services critiques qui composent le web[113]. Côté client, le modèle *open source* est également bien développé comme le démontre la répartition en parts de marché des navigateurs ; Mozilla Firefox détient en France près d'un tiers du marché en 2014[16]

8.2.2 L'open source est un modèle de développement, pas un modèle économique

Franz Meyer, l'un des dirigeants de Red Hat [18] d'expliquer au quotidien *Le Monde* le paradigme du logiciel libre : "Nous ne vendons pas de logiciels : ils sont tous disponibles en téléchargement gratuitement sur Internet. Notre travail, c'est d'y ajouter un support technique, de la maintenance, des garanties juridiques ou sur la durée de vie."[100]. On déplace donc l'offre vers une offre de services afin d'adapter les outils existant au besoin spécifique des entreprises, tout en bénéficiant des différentes montées en gamme ou des nouvelles fonctionnalités proposées par la communauté.

8.2.3 Les sources de revenus

En terme de coûts, le produit technique brut en tant que tel est gratuit pour l'utilisateur ; le modèle génère alors un profit par une voie différente. Il n'y a pas en réalité un unique *business model* lié à l'open source, et chaque éditeur de solutions peut développer son propre modèle afin de générer des revenus.

Dans le cas d'Android par exemple, le coeur du système d'exploitation est *open source* et repose à son tour sur un noyau Linux, lui même *open source*. La gratuité du système d'exploitation a permis aux constructeurs de téléphones portables d'utiliser massivement ce système tout en se détachant eux même de la conception du système d'exploitation.

Pour sa part, le business modèle pour Google ne repose pas sur la vente de son logiciel mais bien sur son interconnexion avec les autres services de la firme. La distribution massive de l'OS Android permet en effet à Google de collecter plus de données personnelles sur les utilisateurs afin d'affiner sa compréhension et de pouvoir proposer des publicités plus en adéquation leurs habitudes [56], ce qui demeure le coeur des revenus de Google depuis sa création.

18. Red Hat est une société éditant des distributions Linux.

Par ailleurs la mise à disposition d'un portail applicatif, l'*Android market*, qui permet à tous de développer une application pour son smartphone et de la vendre, permet également à Google de récupérer un revenu équivalent à 30% du prix de vente de l'application [17] .

8.2.4 Les sources de coûts

Dans la mesure où le produit technique brut est gratuit, il y a une tendance à l'extrapolation qui consiste à penser que le logiciel libre est gratuit ; cette aphorisme est un non-sens. Le logiciel libre a également un coût pour l'entreprise, mais un coût orienté vers le service. Il y a également un coût certain sur les premières années, lié au changement et à l'éducation des utilisateurs.

Le logiciel libre repose sur un modèle de services et non de vente d'une technologie comme c'est le cas pour les logiciels propriétaires. Les budgets sont de ce fait orientés vers la mise en oeuvre de nouveaux projets et vers l'intégration des différents modules plutôt que vers un coût récurrent de licence. On passe donc d'un modèle de Capex majoritaire à un modèle d'Opex plus en prise réelle avec le niveau d'activité des organisations. D'ailleurs, le choix de l'Open Source dans de nombreuses grandes entreprises, services de l'État ou services publics dépend très largement de cette stratégie d'investissement[110]

Par ailleurs, un des avantages du développement d'une industrie de service basée sur des solutions *open source* peut être perçu dans le fait de ne pas être vérouillé sur un prestataire particulier, comme ce peut être le cas avec des technologies propriétaires. Il y a donc un effet de concurrence plus sain qui devrait permettre aux entreprises spécialisées de proposer des services plus compétitifs et de redoubler d'efforts en termes d'innovation et d'intégration.

8.3 La création d'un terreau industriel fertile

Le développement de solutions libres permet l'élaboration d'un tissus industriel fertile et propice à un développement et à une croissance rapide. De nombreuses entreprises se saisissent de la solution, se l'approprient et la proposent à leurs clients agrémentés de services particuliers et différenciés (paramétrage, monitoring, maintenance, ...). A chaque besoin spécifique du client, un module supplémentaire est ajouté à la solution et proposé à l'ensemble de la communauté. La performance du logiciel ainsi que l'ajout de nouvelles fonctionnalités n'est donc plus laissée à une équipe de développeurs, mais est bien le fait de toute une communauté.

Ce nouveau paradigme d'une industrie tournée principalement vers le service permettrait l'emmergence rapide de solutions logicielles à la fois alternatives mais également adaptables pour chaque entreprise. Le développement de telles solutions permettrait en outre de se détacher des solutions propriétaires existantes (souvent américaines) afin de regagner l'indépendance technologique française.

Un tel modèle a déjà fait ses preuves notamment dans le monde du *Content Management System*[19], où des solutions comme Wordpress[2] ont permi l'emmergence d'une communauté importante qui a participé au développement de la solution logicielle pour en faire la première plateforme CMS avec à son actif 25% en nombre de tous les sites web[70]. Par ailleurs, de nombreuses sociétés se sont développées dans cet écosystème[70], avec pour spécialité le développement de sites Web basés sur cette solution. L'utilisation du logiciel libre permet donc d'abaisser les barrières à l'entrée pour une PME désireuse de se lancer dans cette industrie et favorise clairement l'entrepreunariat et l'innovation.

8.4 La difficulté d'appréhension du logiciel libre dans le domaine de la sécurité

Il est à première vue difficile de concilier sécurité et *open source* dans la mesure où la mise à disposition du code source est souvent perçu comme une vulnérabilité en tant que telle. Cependant, un tel discours tient plus d'une crainte irrationnelle qu'à la réalité, et il suffit pour s'en convaincre de se reporter au principe de Kerchoffs, principes fondamentaux de la sécurité, repris par la maxime de Shannon : "L'adversaire connait le système". Kerchoff explique en effet, que la sécurité d'un système ne peut pas reposer sur son secret, chaque secret étant par défaut un point de cassure.

Un logiciel libre est ainsi contraint à une sécurité *by design* et ne peut se cantonner à faire de la sécurité par l'obscurité, c'est à dire à utiliser le fait que son code source ne soit pas disponible pour considérer que son logiciel est sécurisé. Ce principe est par ailleurs repris par les systèmes de chiffrement grand public RSA et AES, dont les algorithmes mathématiques sont totalement libres et connus et qui servent aujourd'hui de base à la sécurisation de la plupart des communications sur le web et le chiffrement de données confidentielles [20].

Enfin, les méthodes de *reverse engineering* permettent aujourd'hui d'étudier dans le détail le comportement d'un logiciel ou d'un composant en l'analysant lors de son exécution ; dans un tel contexte les méthodes de sécurisation par l'obscurité sont très vite contournées lors de l'étude approfondie du système et ne peuvent alors pas constituer pas une sécurisation suffisante.

Il apparait donc que la sécurité d'un système ne peut pas reposer sur le secret de son fonctionnement ou de son implémentation. C'est probablement ce qui explique que les géants du Web ne sont pas inquiets quant au fait que leurs services soient majoritairement hébergés par des serveurs web *open source*, eux-même installés sur des systèmes d'exploitation *open source*[113].

19. Wikipédia définit Un système de gestion de contenu ou SGC (Content Management System ou CMS) est une famille de logiciels destinés à la conception et à la mise à jour dynamique de sites Web ou d'applications multimédia

20. ces algorithmes sont par exemple utilisés par le protocole SSL/TLS pour la sécurisation du protocole HTTP

8.5 L'auditabilité du code

Le logiciel *open source* a un code qui est par définition auditable. Dans une ère de défiance *post* Snowden, où les entreprises ne savent plus forcément près de qui se tourner ou à qui se confier, la possibilité d'auditer gratuitement le code source de la solution permet d'éviter les faux procès d'intention, et donne la possibilité à tout un chacun de revoir le code à la recherche de vulnérabilités ou de portes dérobées volontairement insérées dans le code.

Un tel process ne garantit cependant en aucun cas l'absence de vulnérabilités et il est inconscient de soutenir que les solutions libres sont de fait forcément sécurisées. Ces solutions restent en effet des solutions complètement susceptibles d'être vulnérables comme tous les autres programmes et il suffit de regarder dans la presse pour s'en convaince[143]. Dès lors, l'ouverture d'un système n'exempt absolument pas la solution logicelle de passer de réguliers audits de sécurité auprès de sociétés spécialisées et indépendante.

8.6 Le contrôle de la solution

Une des difficultés qui réside dans le développement de logiciels *open source* est la traçabilité et le contrôle du code ajouté à la solution par les différents contributeurs. En effet, il est indispensable de contrôler de manière neutre et indépendante chaque modification qui est apportée sur la version en production afin d'éviter l'ajout volontaire d'un code malveillant, ou une erreur de programmation qui engendrerait des problèmes de sécurité importants.

Ce cas de figure s'est par exemple produit dans la distribution Debian [21], lorsque l'une des modifications proposée en septembre 2006 sur le programme *OpenSSL* a eu pour effet de réduire drastiquement l'entropie de clés cryptographiques générées par le programme et les rendant alors prédictibles [22] ; ce programme étant à l'origine de la génération des clés pour un vaste nombre d'autres services, tous ont été affectés, rendant les serveurs particulièrement vulnérables. La vulnérabilité ainsi insérée dans les versions en production a seulement été découverte 2 ans plus tard[31].

8.7 Ne pas perdre le contrôle de son SI

Le schéma "*open source* combiné au développement d'un modèle basé sur le service" n'a pas vocation à devenir une externalisation de l'outil informatique. L'idée est juste d'utiliser des outils de base et de référence qui soient *open source* et qui puissent être déployés et configurés par des sociétés de service afin de correspondre exactement aux besoins de la PME et coller au plus prêt de ses besoins métier ; il est effectivement difficilement concevable de développer une unique solution qui puisse correspondre à l'ensemble des besoins métier de l'intégralité des PME ; il est donc primordial d'avoir un coeur de solution assez modulable et *open source* afin que les sociétés de service proposant du développement propre puissent intégrer les nouveaux modules à la solution existante.

21. Debian est une distribution Linux
22. Cette anomalie porte la référence CVE-2008-0166

Perdre le contrôle de son système d'information pour une entreprise est un réel danger, et il faudra prendre garde en permanence, autant que faire se peut de garder dans l'entreprise une MOA et un contrôle fort sur l'intégralité des solutions utilisées. Il devient alors possible de sous traiter et d'externaliser une partie des développements et mise en oeuvre de solutions mais au prix d'un contrôle fort et d'une relation de contrôle privilégiée à la fois avec le prestataire et la solution déployée.

8.8 La nécessité de la confiance

La question de la confiance est la question de fond qui sous tend tous les équilibres dans l'univers de la cybersécurité. Il est primorial de faire confiance à la fois à la solution technique mise en oeuvre et qui protège le système d'information d'intrusions externes, mais il est également particulièrement important de faire totalement confiance au prestataire qui déploie la solution technique et qui l'adapte aux besoins de l'entreprise.

Un des points positifs de l'*open source* est la possible mise en concurrence des différentes entreprises de service sur la notion même de confiance. Effectivement, la perte de confiance globale vis à vis d'une société entrainerait son dépôt de bilan rapide, dans la mesure où il n'existe pas de rente technologique ; les entreprises auraient donc tout intérêt à mettre en oeuvre toutes les mesures possibles afin de renforcer la confiance de leur client. Contrairement à une solution propriétaire, où le client est souvent techniquement contraint de travailler avec la même entreprise (pour ne pas subir les coûts d'un redéveloppement complet de la solution auprès d'une autre entreprise), l'utilisation de solutions *open source* permet à tout un ensemble d'entreprises de travailler sur le même coeur technique. Il n'y a donc plus dépendance à un auditeur, avec des ressources rares donc chères.

Une piste qui pourrait alors être explorée, compte tenu de la nécessité absolue de confiance, est l'existence d'un moyen d'objectiver le niveau de confiance que l'on peut légitimement accorder à une entreprise où une solution technique ; cette objectivation pourrait par exemple être faite au travers d'un processus particulier de labellisation.

C'est d'ailleurs le parti pris de l'ANSSI, qui s'est lancé récemment dans une entreprise de labellisation de "prestataires de confiance" jugés tout autant sur leurs capacités et leur qualité technique que sur la confiance que l'on peut leur accorder vis à vis de la sensibilité des informations traitées.

Le décret n° 2010-112 du 2 février 2010 (article 4) prévoit en ce sens que le recours à des prestataires de services de confiance qualifiés soit la règle générale pour les administrations, les exceptions devant être justifiées ; l'Etat montrant donc le chemin à prendre.

9 Le renforcement de la demande au travers de la commande publique

La prise en compte de la thématique cybersécurité par les PME ne saurait s'insérer dans un dispositif descendant et autoritaire, c'est à dire imposé par l'Etat au moyen de normes et législations. Le *ras le bol* fiscal constaté, ainsi que la dégradation du climat de confiance entre entreprises et Etat[129] imposent donc de trouver une voie alternative pour l'évolution de la prise en compte des enjeux liés à la cybersécurité. C'est ainsi une démarche incitative reposant sur une approche économique qui a été présentée, en complément du soutien de l'Etat à l'emmergence d'une offre *open source*. Ce soutien peut par exemple s'exprimer par le renforcement de la prise de conscience des enjeux de cybersécurité au sein de ses différentes administrations, l'Etat montrant ainsi la voie à prendre et donnant l'exemple.

9.1 Les collectivités territoriales présentent une structure similaire à celle des PME

Dans toute la suite, L'Etat est compris dans sa formulation la plus étendue, c'est à dire en intégrant les fonctions publiques d'Etat, territoriale et hospitalière. C'est donc la sensibilité de structures comme les administrations centrales, les services déconcentrés, les EPA (Etablissement public à caractère administratif) et ODAC (organismes divers d'administration centrale), les collectivités territoriales ainsi que leurs établissements publics, ou les établissements publics de santé qui sera étudié.

A cet égard, de nombreuses structures présentent une organisation, une taille, un mode d'intervention et une sensibilité aux enjeux de cybersécurité sensiblement équivalente à celle observée par les PME.

Cible d'organisations malveillantes Or, l'actualité démontrent que les établissements de santé sont désormais également ciblés par la cybercriminalité, car tout comme les PME, ils présentent un niveau de sécurité informatique moindre, mais dispose d'un nombre important de données personnelles sensibles qui peuvent ensuite être commercialisées. Par ailleurs, leur fonctionnement quotidien et la survie des patients qu'ils hébergent est étroitement dépendant de la disponibilité de nombreux dispositifs connectés, ce qui rajoute une notion de criticité.

Pour ne citer que quelques exemples récemment récemment cités dans la presse, on peut penser aux cas suivants :

- Les communes, les établissements publics de coopération intercommunal [102] [28] [24]
- Les établissements d'enseignements [75] [25] [21]
- Les établissements publics de santé, et établissements sociaux et médicaux sociaux : Centres Hospitaliers Universitaires, mais aussi les hôpitaux ruraux, les maisons de soin, celles de retraite, les établissements de soins spécialisés,

9.1.1 Illustration par le cas des établissements de santé

A l'hôpital psychiatrique de Villejuif par exemple, ce sont les dossiers de près de 400 malades qui ont été modifiés après une intrusion informatique[49] , ce qui appelle à s'interroger sur le suivi des posologies ou interventions programmées.

Outre Atlantique, les établissements de santé ne sont pas en reste puisque la société *Community Health Systems*, qui gère près de 206 hôpitaux dans 29 Etats aux Etats-Unis a annoncé dans un document transmis en août 2014 à l'US Securities & Exchange Commission[30] avoir été la cible d'un groupe de hackers chinois. Ceux-ci seraient parvenus à mettre la main sur les données personnelles de quatre millions et demi de patients, amenant à plus de six millions le nombre d'Etats-Uniens personnellement identifiables au moyen de données dérobées lors les sept premiers mois 2014 [118] et à vingt-et-un millions le nombre de patients affectés par une violation de leurs données personnelles depuis 2009[74].

Victimes de négligence Au delà du risque cyber criminel, c'est également le risque de cyber fuite qui touche de plus en plus les centres de santé.

En 2013 par exemple, ce sont (entre autres) les données médicales de patients de l'hôpital de Marseille [59] qui s'étaient ainsi retrouvées en ligne à cause d'erreurs humaines, mais également celles de l'hôpital Foch de Suresnes et du Pôle de santé du Plateau des villes de Clamart et Meudon [74] ou encore du centre hospitalier de Saint Malo [58].

Et pourtant, l'établissement de santé est garant selon les articles Arts. L.1112-1 et R. 1112-7 du Code de Santé Publique de la protection des données personnelles de ses patients ainsi que du secret médical d'après l'article Art. 4 du Code de déontologie ; il s'expose alors, en cas de de fuites de ces données couvertes par le secret médical à de lourdes sanctions pénales et financières.

Une fois de plus et comme analysé avant, ces sanctions financières viennent s'ajouter à la dégradation de l'image de l'établissement auprès de l'opinion publique. Compte tenu de la difficulté financière dans laquelle se trouve les hopitaux français[62] , et compte tenu de la criticité des informations qu'ils traitent au quotidien, il est fondamental que des mesures rapides soient prises dans ce domaine[74].

Début janvier 2014, ce sont les ARS (Agences régionales de la santé) qui ont, à leur tour, été victimes d'un pirate rendant leurs sites web indisponibles pendant plus d'une semaine [94].

En définitive, les attaques vis-à-vis des établissements de santé ont fortement augmenté. L'assureur britannique Beazley en a d'ailleurs fait l'un de ses principaux axes de développement en matière de cyber assurance. Plus de la moitié de son portefeuille client appartenait ainsi au monde de la santé fin 2013[95].

9.1.2 Une sensibilité équivalente aux enjeux de cybersécurité

En outre, une étude réalisée en 2013 auprès de plus 1500 collectivités territoriales, par la Région de Gendarmerie Nord associée au Conseil Régional du Nord-Pas de Calais [72] a conclu à la très faible prise en compte de la sécurité au sein des systèmes d'information de ces acteurs. Plus grave encore : les obligations légales à mettre en oeuvre sont dans une grande majorité ignorées des décideurs et responsables.

Or comme vu précédemment [23], le fait de ne pas mettre en place les obligations légales empêche bien souvent, lors d'évènements criminels, d'entamer des poursuites judiciaires, laissant ainsi impuni les attaques perpétrées contre les systèmes de l'Etat.

9.2 Intégrer la cyber sécurité au sein de l'Etat

Face à ce double constat, deux axes d'action nous apparaissent comme devant être privilégiés.

En préambule, il parait important de souligner que toute politique tangible de sécurité ne peut être mise en oeuvre efficacement que si elle implique l'ensemble des agents, et qu'elle obtient en amont un soutien politique fort de la part de l'exécutif.

9.2.1 Intégrer la cyber sécurité dès la conception des nouveaux projets

Ceci étant précisé, les entités étatiques doivent absolument intégrer le Référentiel Général de Sécurité (RGS) [14] dans leur démarche de sécurisation des systèmes d'information, et dans leur offre de services publics dématérialisés.

Le Référentiel Général de Sécurité est un document co-produit par l'ANSSI et le SGMAP qui propose une suite de recommandations et de bonnes pratiques afin que l'administration soit en mesure de construire son système d'information et ses applications de manière la plus sécurisée possible.

Le Référentiel général de sécurité (RGS) est créé par l'article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Sa version initiale (la version v.1.0) a été rendue officielle par arrêté du Premier ministre en date du 6 mai 2010 ; une version 2.0, publiée par arrêté du Premier ministre du 13 juin 2014, est applicable à partir du 1er juillet 2014.

Afin d'entrer en conformité avec ce référentiel, toutes les administrations doivent désormais valider les cinq étapes suivantes, prévues par le décret 2010-112 du 2 février 2010, pour tous les nouveaux projets :

- réalisation d'une analyse des risques(art. 3 al. 1) ;
- définition des objectifs de sécurité(art. 3 al. 2) ;

23. voir

– choix et mise en oeuvre des mesures appropriées de protection et de défense du SI(art. 3 al. 3) ;
– homologation de sécurité du système d'information(art.5) ;
– suivi opérationnel de la sécurité du SI.

Cette démarche rationnelle a ainsi pour objectif de faire rentrer la sécurité dans les composantes de base de la construction d'une application ou d'un système, en fonction des risques et des menaces qui pèsent réellement sur ce système.

De plus, la complexité des services numériques rend généralement nécessaire l'externalisation et l'appel aux entreprises du secteur privé. L'administration rédige donc un cahier des charges dans le cadre d'une procédure dite d'appel d'offres européen. Lors du dépouillement de cet appel d'offre, les propositions des différentes sociétés de prestataires sont alors notées en fonction de critères *objectifs* afin de sélectionner celle qui répond le mieux au besoin de l'administration. A date, ce sont les aspects fonctionnels mais surtout financiers qui sont discriminants. Il convient désormais d'ajouter des clauses relatives à la sécurité.

Il apparait également fondamental pour l'administration d'adosser au cahier des charges des procédures de contrôle et de suivi afin de s'assurer du niveau de sécurité des solutions déployées.

Enfin, la sensibilisation du personnel est primordiale sur les questions de cybersécurité, en particulier pour les agents en relation avec les applications déployées afin qu'ils soient en mesure d'adopter un comportement éclairé pour prévenir ou détecter une tentative d'intrusion ou de vol de données.

9.2.2 Sécurisation des systèmes étatiques

Une fois cette orientation acquise pour le développement d'applications, l'administration doit pouvoir formaliser le choix d'outils dont la fonction serait d'améliorer la sécurité de ses propres systèmes ; son choix pourrait alors basculer vers des solutions de sécurité labellisées par l'ANSSI, ou par un prestataire de confiance, voire souveraines.

Afin que cette pratique soit rendue possible au regard du Code des Marchés Publics, le gouvernement a donc tout intérêt à mettre en oeuvre une transposition rapide et adaptée des directives européennes « Marchés Publics » du 28 mars 2014.

Celles-ci prévoient en effet d'élargir le recours à la procédure dite de marché négocié, tout en introduisant la possibilité de critères spécifiques discriminants au sein du cahier des charges (clauses sociales, environnementales, et par extension, sécuritaires).

Cette appropriation de la thématique par l'administration aurait également un rôle d'amorçage et d'entraînement de la demande auprès des entreprises intervenant dans le champs de la cybersécurité. En effet, si les grandes entreprises sont pour l'essentiel couvertes par des dispositifs personnalisés associés à des contrats assurantiels, les *majors* de la cybersécurité sont aujourd'hui peu enclines à s'intéresser au public des PME. Trop granulaire et disparate, le tissu des PME apparaît en effet difficile à adresser, et exigeant, pour un segment de valeur-ajoutée moindre que celui des grandes entreprises ou ETI.

La demande exercée via la commande publique pourrait ainsi conduire des petites / moyennes entreprises du secteur de la cybersécurité à se concentrer afin de proposer des offres agiles et adaptées à ce nouveau public. Afin de favoriser l'emmergence rapide d'une offre adaptée, l'Etat pourrait alors s'engager à préférer des solutions *open source*.

10 L'Etat doit poursuivre son entreprise de sensibilisation et renforcer les dispositifs de formation

Les entretiens et rencontres menés autour de la thématique approfondie dans cette étude ont permis d'appréhender la très grande diversité des institutions étatiques intervenant dans le champ de la cybersécurité et dont l'une des fonctions principales s'articule autour de la sensibilisation du tissu entrepreneurial aux enjeux de cybersécurité, ainsi que dans la mise à disposition de ressources et d'outils, dans une volonté au long terme de progressivement élever le niveau moyen de connaissance du sujet.

Cet engagement dans la sensibilisation doit cependant être supléé par un axe de formation plus spécifique afin de répondre à un autre impératif détecté au détour des échanges : si de nombreux acteurs déclarés gravitent dans la sphère de la cybersécurité française, les grands groupes spécialisées peinent à recruter des profils compétents. Or il s'agit d'un secteur en pleine croissance où les positions sont loin d'être établies sur la scène internationale. La France dispose en conséquence d'une carte à jouer, si elle est en mesure de capitaliser sur ses parcours scientifiques d'excellence, dont il s'agirait d'orienter une partie de façon plus spécifique vers ces domaines.

10.1 Une offre de sensibilisation ramifiée

Dans son agencement actuel, l'action de l'Etat français s'articule assez classiquement entre d'une part, un rôle stratégique exercé par l'administration centrale, et celui plus opérationnel reposant sur une très grande diversité d'acteurs déconcentrés. On observe par exemple au sein de l'administration centrale un morcellement des compétences, chaque entité intervenant globalement de façon indépendante des autres, et en rapport avec le coeur de métier du ministère, ou de sa direction générale de rattachement.

10.1.1 L'ANSSI

En premier lieu, l'Agence Nationale de la Sécurité des Systèmes d'Information, crée par le décret n° 2009-834 du 7 juillet 2009 (Journal officiel du 8 juillet 2009), sous la forme d'un service à compétence nationale, fait suite à la publication, le 17 juin 2008, du Livre blanc sur la défense et la sécurité nationale ; il s'agit de l'autorité nationale en matière de sécurité et de défense des système d'information. L'ANSSI, rattachée au Secrétaire général de la défense et de la sécurité nationale, définit la politique générale de sécurité des systèmes d'information de l'Etat, et propose des règles à appliquer pour la protection des systèmes d'information des opérateurs d'importance vitale, ainsi qu'à leurs fournisseurs de premier rang. L'ANSSI agit au niveau national, et à l'exclusion du champs militaire, il s'agit de la structure la mieux dotée en moyens humains et en technicité. Le rapport annexé à la LPM prévoit par exemple un renforcement sensible des moyens humains de l'ANSSI, qui devront atteindre 500 agents en 2015

Cependant, l'exercice de ses compétences s'effectue sans autorité hiérarchique administrative, ni possibilité évidente de démultiplication locale de son action, surtout parisienne. Récente, son rayon d'action s'est principalement étendu aux états-majors des grandes entreprises, mais faute de relais locaux, ses messages peinent à franchir les limites territoriales du bassin parisien.

10.1.2 La D2IE

Autre acteur de niveau central, la Délégation Interministérielle à l'Intelligence Economique (D2IE) intervient dans le cadre plus général de l'intelligence et la sûreté économique. Rattachée au Secrétariat Général du Gouvernement, elle anime une démarche de sensibilisation des acteurs économiques mais son action demeure assez diffuse du fait de moyens très resserrés.

En coordination avec d'autres acteurs institutionnels, dont l'ANSSI, elle propose depuis le début de l'année 2014 un outil de diagnostic DIESE permettant aux entreprises d'auto-évaluer le degré d'exposition de l'entreprise.

10.1.3 La DGCIS

Côté soutien à une politique de l'offre, la Direction Générale du Commerce, de l'Industrie et des Services (DGCIS) placée sous l'autorité du ministre au redressement productif, intervient dans le cadre du financement des programmes d'investissement d'avenir (PIA), et des 34 plans pour la nouvelle France industrielle [109].

Ses initiatives ont pour objectif, pour le cas qui nous concerne, de faire émerger et croître un biotope économique autour de solutions de cybersécurité. C'est l'une des rares directions à disposer de ressources propres pouvant être affectées directement au financement d'initiatives privées. Ce soutien aux politiques industrielles est réalisé soit via le mécanisme d'avance remboursables, soit par l'intermédiaire de la Banque Publique d'Investissement (BPI) et la Caisse des Dépôts et Consignation (CDC) au travers d'un fonds visant à favoriser l'agrégation de start-ups identifiées comme pertinentes.

10.1.4 DGGN, DGSI, DPSD, ...

Enfin différentes directions générales interviennent dans le champs particulier et granulaire de la sécurité et sûreté du territoire français. Elles n'abordent généralement la cybercriminalité que de façon connexe à leur coeur de métier. Cependant la Direction Générale de la Gendarmerie Nationale (DGGN) et notamment sa communauté N-Tech, et la Direction Générale à la Sécurité Intérieure (DGSI) se sont récemment réorganisées afin d'en faire un axe majeur de leurs interventions.

Leurs actions portent essentiellement sur la sensibilisation des professionnels, mais également des particuliers et administrations au niveau déconcentré. Ils prennent appui sur les relais locaux (Chambres consulaires, organisations syndicales, associations,...) afin de répondre à une triple finalité : éducative, défensive et juridique.

A noter également la Direction à la Protection et à la Sécurité de la Défense (DPSD) qui s'intéresse spécifiquement au tissu industriel à des fins stratégiques militaires.

10.1.5 Une entité pour les gouverner toutes

Globalement, chaque institution intervient efficacement au regard des missions et moyens qui lui ont été confiés. En revanche, il n'existe à la connaissance des auteurs de la présente étude, aucun dispositif permettant de disposer d'une vision agrégée des différentes actions menées.

Impossible dès lors de faire le lien entre d'un côté la mesure des incidents afférents à la cybercriminalité, ceux qui se traduiront par une suite judiciaire, et à la mesure de cet état de lieux, de concrètement déterminer l'effet d'une politique de prévention.

En conséquence, l'Etat gagnerait à une meilleure coordination des efforts dans le cadre d'une stratégie globale pilotée par le Secrétariat du Gouvernement, plutôt qu'à un foisonnement des actions individuelles. La double composante Défense et Economie ne doit pas occulter la finalité qui est bien de contribuer à ce que nos acteurs économiques et industriels réhaussent leur niveau global de sécurité afin de péreniser leur situation.

L'ANSSI pourrait se voir confier les délégations correspondantes, au regard de son périmètre actuel, de son action à cheval entre le monde civil et militaire. Une condition d'efficacité à ce leardership serait qu'y soient détachées des personnes représentatives de chacune des administrations centrales considérées.

Il conviendrait ainsi de créer cette nouvelle "force" (sans réellement créer une structure à part entière) sous l'autorité de l'ANSSI et qui regrouperait les principaux acteurs locaux afin de s'assurer de la cohérence et de l'homogénéité des actions de sensibilisation et de prévention. Une externalité positive serait alors de pouvoir agréger au niveau national les données et retours d'expérience qui sont aujourd'hui conservés par administration.

Enfin les travaux de sensibilisation, les idées, les démontrations issus de cette nouvelle entité pourraient être diffusés par des vecteurs décentralisés qui agissent au plus près des entreprises et dont les éléments de langage sont plus aptes à toucher les entreprises ; on peut alors penser à des structures telles que le Medef ou la CGPME.

10.2 Contribuer à faire évoluer le rapport de l'individu à l'outil informatique

10.2.1 Le rôle de l'éducation nationale

L'appréhension des fonctionnalités offertes par l'outil numérique (tablettes, smartphones,...) semble, comme de coutume, instinctive pour les jeunes générations. En revanche, l'apprentissage des risques associés à ces *facilités* est loin d'être

évident, d'autant plus que ceux-ci sont en grande partie ignorés par leurs aînés et parents.

D'où l'identification d'un acteur qui nous semble le mieux adapté afin de porter le message à l'attention des entrepreneurs de demain : le ministère de l'Education Nationale. Il n'existe au jour de la publication du présent mémoire, aucune action qui soit pilotée au niveau national par ce ministère sur la thématique Cybersécurité.

Ce constat est d'autant plus surprenant que de nombreuses actions de sensibilisation sont par ailleurs menées en liaison avec les circonscriptions locales de gendarmerie ou de police, autour de risques aussi divers que ceux en lien avec la circulation ou l'usage de stupéfiants. Les intervenants y présentent ainsi les dangers et punitions relatifs aux infractions et délits afférents.

Aussi, il nous semblerait utile que le ministère de l'Education Nationale s'empare de ce sujet, et l'intègre dans ses objectifs d'éducation dès les premières années du cycle primaire. En effet, les enfants recourent très tôt à l'outil numérique, et la sensibilisation nous semble plus utile dès leur jeune âge. Une seconde vaccination préventive au collège, et donc à l'âge des premiers usages des réseaux sociaux, permettrait de compléter le dispositif.

Enfin, dans tous les cours d'informatique dispensés, des règles de bonnes pratiques devraient être enseignées et une sensibilisation aux questions de sécurité devrait faire partie des acquis fondamentaux.

En outre, et afin d'être efficace dans les plus brefs délais, le message devrait être relayé de façon plus systématique à l'attention de la population française. A cet égard une campagne de communication pourrait gagner à suivre la voie empruntée par la Sécurité Routière, ou plus récemment par le Conseil Supérieur de l'Audiovisuel, en saisissant l'esprit collectif par des images chocs.

10.2.2 Mise en place d'un parcours professionnel qualifiant

La sensibilisation de citoyens éveillés aux dangers de la cybercriminalité est une nécessité. Elle ne doit toutefois pas occulter la formation d'experts dont le manque se fait ressentir par la profession.

Un cruel besoin d'experts Jean-Pierre Quémard, le président de l'Alliance pour la confiance numérique, évalue les besoins entre 2000 et 4000 personnes par an , sur un marché français dont la demande croit de 5 à 10 % par an [108] quand le système français ne délivre que 500 diplômés ayant suivi une formation en cybersécurité par an.

Un premier constat s'impose : tout d'abord, il serait étonnant de ne répondre à l'attente de l'un des rares secteurs économiques à ne pas souffrir de la crise actuelle. De nombreux ingénieurs en formation ou étudiants des filières scientifiques en université pourraient être tentés par cette voie prometteuse, à supposer que l'Etat ou les entreprises demandeuses sachent les y orienter.

La création d'une filière d'excellence En second lieu, les auteurs du présent rapport sont convaincus que la poursuite du développement de formations qualifiantes est un prérequis indispensable pour que l'Etat français maintienne une certaine indépendance dans la maîtrise du sujet.

Une voie à retenir pourrait être celle mise en oeuvre par le GCHQ britannique, consistant en la validation qualitative des enseignements de grande qualité, une sorte de labellisation de la formation [22]. Un tel processus permettrait surement de favoriser l'emmergence d'une filière d'excellence de la cybersécurité en s'attachant à recruter sur concours des profils particuliers.

Recrutement de profils atypiques au sein de l'état Ces formations contribueront à répondre aux besoins civils et économiques, mais ne doivent pas s'avérer exclusives d'autres voies de recrutement, notamment vis à vis de profils atypiques. Deux verrous ont été identifiés atténuant cette possibilité : le premier porte sur la capacité juridique offerte aux administrations de pouvoir recruter en dehors du régime des concours communs ; le second étant la gageure de pouvoir intéresser des profils d'experts éthiques.

S'agissant du premier point, le ministère de la Défense a ouvert la voie en s'engageant dans le recrutement de profils particuliers afin d'étoffer les équipes de son pôle d'excellence en cybersécurité Rennais.

Mais les autres administrations se fondent plus généralement sur le régime de concours en vigueur au sein des trois fonctions publiques afin de distinguer les profils potentiels. Or le recrutement de profils très spécifiques est aujourd'hui possible au regard du droit existant, et de nature à répondre aux exigences des contrôleurs budgétaires et comptables ministériels.

Concernant l'attrait de la fonction publique, une mesure pourrait consister à éveiller la communauté des experts, au travers de plusieurs *challenges* à l'image de celui de l'ANSSI qui consistait en une énigme cachée dans le logo de cette administration.

Ces défis sont donc un excellent moyen pour entrer en contact et dénicher des perles rares, invisibles des systèmes de recrutement classiques.

Il apparait au terme de cette analyse que les petites et moyennes entreprises, si elles jouent un rôle clé dans l'activité économique du pays n'ont pas pris la mesure des nouveaux risques induits par les formidables fonctionnalités rendues possibles par les nouvelles technologies. Leur manque de sensibilisation par rapport aux enjeux de cybersécurité, combiné au manque de moyens alloués sur le sujet mais également à l'incapacité de l'ANSSI à les accompagner font de ces entreprises des cibles de choix dans les campagnes de cyber attaques. Que ce soit pour leur propriété intellectuelle, pour l'utilisation de leurs ressources ou pour bénéficier de l'accès privilégié dont elles jouissent vers un grand groupe pour lequel elles sous traitent une partie de l'activité, les PME sont ainsi souvent confrontées à des situations dans lesquelles un programme tente de prendre la main sur leur système d'information.

Il est donc fondamental d'adopter avec rigueur un comportement averti et responsable tel que proposé par le guide d'hygiène comportemental élémentaire et qui se décline en une série de règles et de recommandations :

- **Règle 1 :** Un système peut être compromis et ce même si aucun comportement suspect n'est détecté ni par l'utilisateur ni par un autre autre programme (type antivirus).
- **Règle 2 :** Une PME, ou un particulier, peut se retrouver au centre d'une campagne d'espionnage, et ce même sans en être la cible principale. Elle devient alors le vecteur d'intrusion.
- **Règle 3 :** Une PME, ou un particulier, peut se retrouver au centre d'une campagne de sabotage même sans en être la cible principale. Elle devient alors le vecteur d'intrusion.
- **Règle 4 :** Un système relié à internet est forcément une cible pour une organisation malveillante : soit pour les données qu'il contient, soit pour la ressource qu'il constitue.
- **Règle 5 :** Les attaques non ciblées peuvent souvent être évitées au moyen de mesures simples d'hygiène comportementale
- **Règle 6 :** Un email, à moins d'être signé par un protocole cryptographique, ne peut jamais être réputé fiable
- **Règle 7 :** Il y a schématiquement 2 manières d'être infecté :
  - En lançant soi-même un fichier exécutable contenant une portion de code malicieux
  - Parcequ'un code malicieux exploite une faiblesse dans un système ou une application qui lui permet de charger en mémoire et d'exécuter un *payload*.
- **Règle 8 :** Un antivirus, bien qu'indispensable n'est pas une solution miracle aux enjeux de sécurité informatique ; sa présence ne doit en aucun cas justifier des comportements risqués.
- **Règle 9 :** Le cloud computing n'est pas une solution miracle aux enjeux de sécurité et ne réduit qu'une partie de la surface d'attaque ; les applications ainsi que les clients finals restent des cibles tout autant exposées. Par ailleurs, la délocalisation de son informatique ne peut être envisagée qu'auprès de prestataires de confiance.

- **Recommandation 1 :** Le meilleur moyen de lutter contre les attaques de type *drive by download* est d'avoir un système systématiquement et rigoureusement à jour [24] (aussi bien le système que l'intégralité des programmes tiers) et de minimiser la surface d'exposition en n'installant que les programmes strictement nécessaires et en n'activant que les modules complémentaires réellement utilisés.
- **Recommandation 2 :** Il convient de désinstaller Java, vecteur d'intrusion particulièrement utilisé.
- **Recommandation 3 :** Il convient de désactiver l'*autorun* (ou fonctionnalité équivalente sur les autres systèmes d'exploitation) afin d'éviter tout comportement automatique du système lors de la détection d'un nouveau périphérique.
- **Recommandation 4 :** Il convient de désactiver l'*autoplay* (ou mécanisme équivalent sur les autres systèmes d'exploitation)afin d'éviter tout comportement automatique du système lors de la détection d'un nouveau périphérique.
- **Recommandation 5 :** Les clés USB insérés dans les systèmes de l'entreprise doivent être la propriété de l'entreprise et ne doivent en aucun cas venir de l'extérieur ou avoir été branchées sur un système étranger.
- **Recommandation 6 :** Les clés USB doivent impérativement être chiffrées
- **Recommandation 7 :** On ne télécharge que les applications strictement nécessaires au bon fonctionnement opérationnel de l'activité. Les applications sont exclusivement téléchargées depuis les sites officiels. La vérification des empreintes cryptographiques avant installation du logiciel téléchargé est nécessaire afin de s'assurer que la version téléchargée est bien conforme à la version officielle.
- **Recommandation 8 :** L'utilisation de réseaux P2P est proscrite.
- **Recommandation 9 :** Effectuer des backups réguliers de son système est une bonne pratique.
- **Recommandation 10 :** L'utilisation de Wifi libre ouvert ou protégé avec le protocole WEP est à éviter. Elle pourra être tolérée si et seulement si :
  - Le système est connecté en VPN à un réseau de confiance (réseau personnel ou de l'entreprise)
  - Les flux sont dirigés vers un proxy au travers d'un canal sécurisé (type ssh)

  Dans tous les cas, on lui préfèrera l'utilisation du protocole WPA2 (ou WPA CCMP) avec utilisation lorsque cela est possible d'un serveur d'authentification Radius (802.1x EAP-TLS)
- **Recommandation 11 :** Chiffrer l'intégralité de son disque dur est une bonne pratique
- **Recommandation 12 :** La construction d'applications web en interne comme en externe doit être suivie par des prestataires de confiance et la sécurité de ces applications doit être auditée de manière régulière.

24. Chaque système d'exploitation propose des outils afin de faire des mises à jour de manière automatique

Ce rapport propose également la mise en place d'une démarche incitative à la prise en compte des enjeux liés à la cyber sécurité au travers de deux leviers économiques fondamentaux :

- La Banque de France dans son rôle d'Organisme Evaluateur Externe de Crédits
- Les assureurs dans leur rôle de soutien à la continuité d'activité suite à la survenue d'un incident.

Dès lors, la direction des entreprises à la Banque de France pourrait inclure dans sa matrice de cotation des risques un aspect lié à la prise en compte des risques cyber, dans la mesure où ces derniers ont un rapport direct avec la capacité pour une entreprise d'honorer ses engagements financiers à moyen terme. L'activité d'une entreprise étant de nos jours souvent dépendante de l'outil informatique, le manque de disponibilité de ce dernier pourrait en effet causer des dégats financiers considérables qui viendrait s'ajouter au déficit de confiance résultant de la compromission des systèmes ou au vol de la propriété intellectuelle qu'il contenait.

L'indice de sécurité de l'entreprise serait alors calculé au moyen d'un outil élaboré en partenariat avec les institutions dont une partie du coeur de métier s'oriente vers les questions de sécurité économique (comme l'ANSSI, la D2IE, la DGSI et la DGGN) et pourrait par exemple s'appuyer sur l'outil DIESE mis en place par la D2IE et développé en collaboration avec l'ANSSI. La Banque de France aurait alors pour mission de pondérer cet indice afin qu'il s'intègre dans sa matrice de cotation des risques dans un modèle aussi cohérent que possible avec la projection de la réalité dont elle dispose.

Par ailleurs, dans son rôle pédagogique auprès des entreprises, la Banque de France, lorsqu'elle se déplace auprès d'elles, pourrait diffuser des éléments de langages englobant de ces nouveaux risques et ainsi se faire le vecteur de certaines bonnes pratiques, comme le guide d'hygiène comportemental proposé dans cette étude.

Les compagnies d'assurance ont également un rôle clé à jouer pour favoriser une large prise en compte des enjeux liés à la cybersécurité ; en proposant des polices d'assurance spécialisées dans les risques cyber et dont le montant de la police dépendrait des mesures mises en place afin de réduire le spectre des vulnérabilités des systèmes et des applications métier, la compagnie d'assurance propose à chacun de ses clients de trouver son optimum économique. Dans la mesure où la mise en place de simples mesures d'hygiène informatique et le respect des règles d'hygiène comportementales proposées dans cette étude permettent de réduire de manière significative l'exposition de l'entreprise à un coût faible, un tel procédé permettra de favoriser l'emmergence d'une attitude éclairée, à faible coût.

Compte tenu de l'impressionnante croissance des dégats financiers causés par la compromission de systèmes, et pour se protéger de la multiplication des plaintes de particuliers liées à la compromission de leurs données hébergées chez des prestataires, le cadre devient très favorable au développement de ce marché,

à l'image du marché américain qui connait une croissance à deux chiffres depuis quelques années.

Enfin, le développement d'une telle offre, permettrait d'obtenir des statistiques plus précises et probablement plus en phase avec la réalité concernant le nombre d'attaques dont sont victimes les PME, ainsi que les protocoles opératoires utilisés par les cyber criminels, en conditionnant l'activation du procédé assurantiel au dépot de plaintes.

Ces deux leviers prendront bien soin d'exiger l'intégration d'une partie liée à la sécurité des systèmes d'information lors d'appels d'offres pour le déploiement de nouvelles applications métiers ou de nouveaux composants d'informatique industrielle.

Au delà de ces démarches purement économiques, d'autres acteurs, comme l'Etat pourraient contribuer à l'amélioration globale du niveau de sécurité des PME en focalisant une partie de leurs investissements vers le soutien à l'emmergence de solutions *open source*.

Le développement de telles solutions permettrait ainsi la création d'un terreau fertile susceptible de créer un environnement propice à la croissance d'offres de service compétitives autour de logiciels de qualité. Un tel scénario, en plus de converger avec une volonté de retrouver l'indépendance technologique permettrait, avec de faibles barrières à l'entrée, la création d'une fourmillière de sociétés spécialisées dans la sécurité des sytstèmes d'information ainsi que dans le développement et le paramétrage de certaines solutions techniques.

La problématique de la confiance, aussi bien dans une solution que dans un prestataire se posera alors et devra tenter d'être objectivée par un cadre élaboré par l'ANSSI ainsi que des mécanismes de certification rigoureux.

L'Etat, au travers de toutes ses institutions et collectivités dont une grande partie possède une structure et une sensibilité similaire aux PME, s'attachera alors à sélectionner exclusivement des solutions en accord avec ces principes, tout en incluant dans chacun de ses appels d'offres ou ses projets de développement applicatif un volet axé sur la cybersécurité des solutions, comme préconisé par le Référentiel Général de Sécurité.

Enfin, il apparait fondamental de favoriser la formation de potentiels à haute valeur ajoutée en proposant la création de parcours universitaires qualifiants. La France pourrait alors tirer profit de l'excellence de son poulailler scientifique et de sa formation supérieure dans les sciences mathématiques. Un tel comportement permettrait de s'assurer des ressources humaines nécessaires dans un coeur de métier qui en plus d'avoir des conséquences économiques majeures devient un atout pour des questions qui touchent au coeur de la souveraineté.

Références

[1] Blog. http://rbnexploit.blogspot.fr/.

[2] Site Web. http://fr.wordpress.org/.

[3] Avis du certa. Site Web du CERTA. http://www.cert.ssi.gouv.fr/site/CERTA-2010-AVI-088/.

[4] Creating an autorun-enabled application. Site web officiel Microsoft. http://msdn.microsoft.com/en-us/library/windows/desktop/cc144206%28v=vs.85%29.aspx.

[5] Cve details, acrobat reader vulnerability statistics. Site web. http://www.cvedetails.com/product/497/Adobe-Acrobat-Reader.html?vendor_id=53.

[6] Fin de support windows xp et office 2003 le 8 avril 2014. Site Officiel Support Microsoft. http://support.microsoft.com/kb/2982791.

[7] Glossaire portail de la sécurité informatique. Page Web. http://www.securite-informatique.gouv.fr/gp_rubrique33_lettre_C.html.

[8] Ms14-045 : Description of the security update for kernel-mode drivers : August 12, 2014. Blog Officiel Microsoft. http://www.microsoft.com/fr-fr/windows/enterprise/fin-support-XP/default.aspx.

[9] Paris wi-fi accessible dans les jardins parisiens. Page Web. http://www.paris.fr/wifi.

[10] Pole scs. Page Web Officielle du pôle de compétitivité SCS. http://www.pole-scs.org/p%C3%B4le-scs/pr%C3%A9sentation.

[11] Pole tes. Page web officielle du pole de compétitivité TES. http://www.pole-tes.com/le-pole-tes/presentation/.

[12] Procédure de désactivation de la fonction d'exécution automatique dans windows. Site web de support officiel de Microsoft. http://support.microsoft.com/kb/967715/fr.

[13] Reconnaissance des organismes externes d'évaluation de crédit par l'autorité de contrôle prudentiel. Site Internet de la Banque de France. http://acpr.banque-france.fr/communication/communication-a-la-profession/reconnaissance-des-organismes-externes-devaluation-de-credit-par-lautorite-de-contro
html.

[14] Référentiel général de sécurité. Site Web de l'ANSSI. http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/.

[15] Solutions communicantes et sécurisées. Page Web Officielle des Poles de Compétitivité. http://competitivite.gouv.fr/identifier-un-pole/fiche-d-un-pole-555/solutions-communicantes-securisees-14/solutions-communicantes-securisees-17/solutions-communicantes-securisees-18.html?cHash=722e839cc56b70ad7528a4f72ee78e03.

[16] Statcounter global stats. Page web officielle. http://gs.statcounter.com/#browser-FR-monthly-201406-201406-bar.

[17] Transaction fees. Android Developer Help. https://support.google.com/googleplay/android-developer/answer/112622?hl=en.

[18] Transactions electroniques sécurisées. Page Web Officielle des Poles de Compétitivité. http://competitivite.gouv.fr/identifier-un-pole/fiche-d-un-pole-555/transactions-electroniques-securisees-72/transactions-electroniques-securisees-75/transactions-electroniques-securisees-tes-76.html?cHash=ce289002d0275e4abc1ab429224bc949.

[19] Usb rubber ducky, the original keystroke injection tool. Site internet. http://usbrubberducky.com.

[20] Vupen. Site Web. http://www.vupen.com/english/.

[21] Elle pirate la fac pour améliorer ses notes. *Le Figaro*, 01 Juin 2011. http://www.lefigaro.fr/flash-actu/2011/06/01/97001-20110601FILWWW00317-elle-pirate-le-site-de-sa-fac.php.

[22] Developing the cyber experts of the future - gchq certifies master's degrees in cyber security. Site web officiel GCHQ, 1 aout 2014. http://www.gchq.gov.uk/press_and_media/press_releases/pages/gchq-certifies-masters-degrees-in-cyber-security.aspx.

[23] Protéger les entreprises contre les lois américaines. *Les Echos*, 10 Avril 2013. http://www.lesechos.fr/10/04/2013/LesEchos/21414-518-ECH_proteger-les-entreprises-contre-les-lois-americaines.htm.

[24] Le site de la mairie de beaumont-sur-sarthe piraté par des islamistes. *Le Figaro*, 10 Avril 2014. http://www.lefigaro.fr/actualite-france/2014/04/10/01016-20140410ARTFIG00040-le-site-de-la-mairie-de-beaumont-sur-sarthe-pirate-par-des
php.

[25] Il pirate le réseau informatique de son collège pour modifier ses notes. *Le Monde*, 12 janvier 2010. http://www.lemonde.fr/technologies/article/2010/01/12/il-pirate-le-reseau-informatique-de-son-college-pour-modifier-ses-notes_1290475_651865.html.

[26] Logiciels d'auto-évaluation. Page Web, 13 Mai 2014. http://www.intelligence-economique.gouv.fr/methodes-et-outils/logiciels-dauto-evaluation.

[27] Les pme sont des cibles de choix pour les hackers. *Les Echos*, 17 Avril 2013. http://www.lesechos.fr/17/04/2013/LesEchos/21419-111-ECH_les-pme-sont-des-cibles-de-choix-pour-les-hackers.htm.

[28] Le site internet de la mairie de montauban piraté. *Libération*, 17 Janvier 2012. http://www.liberation.fr/politiques/2012/01/17/le-site-internet-de-la-mairie-de-montauban-pirate_789019.

[29] Understanding man-in-the-middle attacks. Site Web, 17 Mars 2010. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html.

[30] Community health systems, inc. FORM 8-K, 18 Aout 2014. http://www.sec.gov/Archives/edgar/data/1108109/000119312514312504/d776541d8k.htm.

[31] Cve-2008-0166. Site Web, 2008. https://security-tracker.debian.org/tracker/CVE-2008-0166.

[32] Notifications de violation de données personnelles : une nouvelle téléprocédure. Site Web Officiel, 23 août 2013. http://www.cnil.fr/linstitution/actualite/article/article/notifications-de-violation-de-donnees-personnelles-une-nouvelle-teleprocedure/.

[33] L'antivirus est mort. *Les Echos*, 5 Mai 2014. http://technologies.lesechos.fr/revue-de-web/l-antivirus-est-mort_a-54-1184.html.

[34] «allianz cyber protect» : pour une protection efficace contre les risques du cyberespace. Communiqué de presse, 5 Septembre 2013. https://www.allianz.ch/public/fr/a_notre_propos/espace_media/communiques_de_presse/communiques_de_presse/2013/05.09.13_cyber_protect.html.

[35] 12ème édition de l'observatoire de l'e-pub du sri, réalisé par pwc, en partenariat avec l'udecam. Site web officiel SRI, 8 Juillet 2014. http://www.sri-france.org/2014/07/08/12eme-edition-de-lobservatoire-de-le-pub-du-sri-realise-par-pwc-en-partenariat-avec-

[36] Operation ghost click. Site Officiel FBI, 9 Novembre 2011. http://www.fbi.gov/news/stories/2011/november/malware_110911.

[37] Simple mail transfer protocol. RFC 821, Aout 1982. http://tools.ietf.org/html/rfc821.

[38] Osx.flashback.k – suffering a slashback – infections down to 270,000. Blog Officiel Symantec, Avril 2012. http://www.symantec.com/connect/blogs/osxflashbackk-suffering-slashback-infections-down-270000.

[39] More details on "operation aurora". Blog Officiel Mc Afee, Janvier 2010. http://blogs.mcafee.com/mcafee-labs/more-details-on-operation-aurora.

[40] Interactive mail access protocol. RFC 1064, Juillet 1988. http://tools.ietf.org/html/rfc1064.

[41] Understanding man-in-the-middle attacks – part2 : Dns spoofing. Site Web, Mars 2010. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part2.html.

[42] Post office protocol. RFC 918, Octobre 1984. https://www.ietf.org/rfc/rfc918.txt.

[43] RACHEL ABRAMS. Target puts data breach costs at 148 million, and forecasts profit drop. *New York Times*, 5 aout 2014. http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html?_r=0.

[44] Camille Adaoust. La cybercriminalité tisse sa toile. *Le Figaro*, 19 juillet 2014. http://www.lefigaro.fr/secteur/high-tech/2014/07/19/

01007-20140719ARTFIG00034-la-cybercriminalite-tisse-sa-toile.php.

[45] AMF. *Rapport 2007 de l'AMF sur les agences de notation, Notation crédit des entreprises, AMF*, 2008. http://www.amf-france.org/technique/multimedia?docId=workspace://SpacesStore/ac935efb-5c88-4a9b-a177-027b27bb540d_fr_1.0_rendition.

[46] ANSSI. *Guide d'hygiène Informatique, ANSSI*, 28 Janvier 2013. http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf.

[47] ANSSI. *Défense et sécurité des systèmes d'information, Stratégie de la France*, Février 2011. http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf.

[48] Damien Bancal. Defacement. Page Web. http://www.zataz.com/category/piratage/defacement/.

[49] Damien Bancal. Piratage des données de l'hôpital psychiatrique de villejuif. Site Web, 1 juillet 2014. http://www.zataz.com/piratage-des-donnees-de-lhopital-psychiatrique-de-villejuif/.

[50] Damien Bancal. Reuters piraté via l'application taboola. Page Web, 24 juin 2014. http://www.zataz.com/reuters-pirate-via-lapplication-taboola/.

[51] Clara Beaudoux. Apple à son tour victime d'une attaque informatique. *France Info*, 19 Fevrier 2013. http://www.franceinfo.fr/high-tech/vie-quotidienne/article/apple-son-tour-victime-d-une-attaque-informatique-231109.

[52] Jean-Marie Bockel. *La cyberdéfense : un enjeu mondial, une priorité nationale*. Rapport d'information 681, 2012. http://www.senat.fr/rap/r11-681/r11-681_mono.html.

[53] Yann Le Brech. La sécurité des clés usb. *Misc*, septembre 2009. http://connect.ed-diamond.com/MISC/MISC-045/La-securite-des-cles-USB.

[54] CEIS. *LES MARCHES NOIRS DE LA CYBERCRIMINALITE*, Juin 2011. http://www.lerti.com/web/public/Les_marches_noirs_de_la_cybercriminalite_Juin_2011.pdf.

[55] CERTA. Cheval de troie. Page Web. http://www.cert.ssi.gouv.fr/site/CERTA-2005-REC-002/.

[56] Jianfeng Lin Arunabha Saha Cheng-Chieh Chao, Zeng Fan. Analysis of google's strategy on android. *x*, x. http://web.stanford.edu/~ccchao1/Business%20Strategy/MS&E%20270%20Android.pdf.

[57] Pierre-André CHIAPPORI. Risque et assurance, 1997. .

[58] Laetitia Clavreul. 375 dossiers d'une clinique de troyes indexés sur google. *Le Monde*, 19 Mars 2013. http://www.lemonde.fr/sante/article/2013/03/19/dans-une-clinique-de-troyes-375-dossiers-indexes-sur-google_1850367_1651302.html.

[59] Laetitia Clavreul. Dossiers de patients sur le net : le secret médical pris en défaut. *Le Monde*, 19 Mars

2013. http://www.lemonde.fr/sante/article/2013/03/19/des-dossiers-medicaux-de-patients-divulgues-sur-internet_1850366_1651302.html.

[60] Olga Kharif Cliff Edwards and Michael Riley. Human errors fuel hacking as test shows nothing stops idiocy. *Bloomberg*, 27 Juin 2011. http://www.bloomberg.com/news/print/2011-06-27/human-errors-fuel-hacking-as-test-shows-nothing-prevents-idiocy.html.

[61] Conseil de l'Europe. *Convention sur la cybercriminalité*, 2001. http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm.

[62] Cours des Comptes. *Rapport sur l'application des lois de financement de la sécurité sociale*, 10 Septembre 2013. http://www.ccomptes.fr/content/download/60167/1493393/version/5/file/rapport_securite_sociale_2013_version_integrale.pdf.

[63] Thiébaut Devergranne. Pourquoi il vous sera impossible de déposer plainte en cas de piratage informatique. Page Web, 25 Avril 2013. http://www.donneespersonnelles.fr/pourquoi-il-vous-sera-impossible-de-deposer-plainte-en-cas-de-piratage-informatique.

[64] DGCIS. *Investissements d'Avenir – Développement de l'Économie Numérique, Coeur de filière numérique, sécurité numérique,*, Octobre 2013. http://investissement-avenir.gouvernement.fr/sites/default/files/user/AAP_COEUR%20DE%20FILIERE_SECURITE%20VF.pdf.

[65] DGFIP - INSEE -DGCIS, base de donnees fiscale et base de données LIFI-DIANE, chiffre de 2010. *Annexe au projet de loi de finances pour 2014, effort financier de l'Etat en faveur des petites et moyennes entreprises.* http://www.performance-publique.budget.gouv.fr/sites/performance_publique/files/farandole/ressources/2014/pap/pdf/jaunes/jaune2014_PME.pdf.

[66] Journal du Net. Fin de windows xp : les entreprises boudent en masse windows 8 et 8.1. Page Web. http://www.journaldunet.com/solutions/dsi/migration-vers-windows-8-8-1-fin-d-xp.shtml.

[67] Journal du Net. Profil-type du responsable sécurité des systèmes d'information. Page Web. http://emploi.journaldunet.com/magazine/1485/.

[68] Philippe Richard Eric Filiol. *Cybercriminalité*. Dunod, 2006.

[69] ESET. Nouvelle vague de ransomware avec la variante "cryptowall". *Global Security Mag*, Juillet 2014. http://www.globalsecuritymag.fr/Nouvelle-vague-de-ransomware-avec,20140704,46130.html.

[70] Tom Ewer. 20 compelling statistics that represent the dominance of wordpress. Blog, 6 avril 2012. http://premium.wpmudev.org/blog/brief-history-of-wordpress-in-numbers/.

[71] FEVAD. Bilan du e-commerce en france : les ventes sur internet franchissent la barre des 50 milliards d'euros en 2013. Communiqué de Presse, 30 Janvier 2014. http://www.fevad.com/espace-presse/bilan-du-e-commerce-en-france-les-ventes-sur-internet-franchissent-la-barre-des-50-m

[72] FIC. *5eme forum international de la cybersécurité, les actes du forum*, 2013. http://www.observatoire-fic.com/wp-content/uploads/2014/01/Actes-du-FIC2013.pdf.

[73] FireEye. *À la recherche de traces numériques :sept indices pour identifier l'auteur d'une cyberattaque avancée*, 2013. http://www.fireeye.com/fr/fr/resources/pdfs/digital-bread-crumbs.pdf.

[74] Alexandra Gavarone. Les établissements de santé français sous-estiment le risque de fuite de données. *Les Echos*, 20 Décembre 2013. http://www.lesechos.fr/idees-debats/cercle/cercle-87346-les-etablissements-de-sante-francais-sous-estiment-le-risque-de-fuite-d php.

[75] Raphaël Gibour. L'université de bourgogne piratée pour la nouvelle année. *Le Figaro*, 3 Janvier 2013. http://etudiant.lefigaro.fr/le-labeducation/actualite/detail/article/l-universite-de-bourgogne-piratee-pour-la-nouvelle-annee-828/.

[76] Dan Goodin. Attackers turn bank of india site into malware bazaar. *The Register*, 1 Septembre 2007. http://www.theregister.co.uk/2007/09/01/bank_of_india_website_takeover/.

[77] Dan Goodin. Flame malware hijacks windows update to spread from pc to pc. Blog Ars Technica, 4 juin 2012. http://arstechnica.com/security/2012/06/flame-malware-hijacks-windows-update-to-propogate/.

[78] Guillaume Grallet. Anonymous : et maintenant à l'assaut de sony et de vivendi ! *Le Point*, 23 Janvier 2012. .

[79] The Radicati Group. *Email Statistics Report, 2014-2018*, 14 Avril 2014. http://www.radicati.com/?p=10644.

[80] Darya Gudkova. *Spam Evolution 2013*. Kaspersky, 23 Janvier 2014. http://media.kaspersky.com/pdf/LK_KSB_2013_spam_EN.pdf.

[81] Jorick GuillaneuF. *La cybercriminalité et les infractions liées à l'utilisation frauduleuse d'Internet : éléments de mesure et d'analyse pour l'année 2012*. Inhesj-Ondrp Rapport 2013, 2013. http://www.inhesj.fr/sites/default/files/files/ondrp_ra-2013/dii_cybercriminalite_cr.pdf.

[82] Teena Hammond. Windows xp : 37% des entreprises us le conservent malgré la fin du support. *ZDNet*, 18 Avril 2014. http://www.zdnet.fr/actualites/windows-xp-37-des-entreprises-us-le-conservent-malgre-la-fin-du-support-39798260.htm.

[83] Charles Haquet. Areva victime d'une attaque informatique de grande ampleur. *L'expansion*, 29 Septembre 2011. http://lexpansion.lexpress.fr/entreprises/areva-victime-d-une-attaque-informatique-de-grande-ampleur_1364967.html.

[84] Antoine Cervoise Jean-Loup Richet. Fraude au clic et dnschanger : l'étude du cas de l'opération ghost click. *Misc*, Mai 2012. http://connect.ed-diamond.com/MISC/MISC-061/Fraude-au-clic-et-DNSChanger-l-etude-du-cas-de-l-operation-Ghost-Click.

[85] Caleb Sima Joel Scambray, Vincent Liu. *HACKING EXPOSED WEB APPLICATIONS, 3rd Edition*, 2010. .

[86] Sylvie Johnsson. Cyber-attaques : après twitter, facebook. *France Info*, 16 Fevrier 2013. http://www.franceinfo.fr/monde/actu/article/cyber-attaques-apres-twitter-facebook-230155.

[87] Journal Officiel. *Article 226-16 Code Pénal*. http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006417955&dateTexte=&categorieLien=cid.

[88] Journal Officiel. *Section 2 : Désignation des opérateurs d'importance vitale, des délégués pour la défense et la sécurité et des points d'importance vitale.* http://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000006182855&cidTexte=LEGITEXT000006071307&dateTexte=20080505.

[89] Journal Officiel. *LOI n° 2014-344 du 17 mars 2014 relative à la consommation (1)*, 17 Mars 2014. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028738036&categorieLien=id.

[90] Journal Officiel. *décret n° 2008-1354 du 18 décembre 2008 relatif aux critères permettant de déterminer la catégorie d'appartenance d'une entreprise pour les besoins de l'analyse statistique et économique*, 18 décembre 2008. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000019961059.

[91] Journal Officiel. *LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*, 18 Décembre 2013. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&dateTexte&categorieLien=id.

[92] Journal Officiel. *loi n° 2004-1484 du 30 décembre 2004 de finances pour 2005, Art 24*, 30 Décembre 2004. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000789373.

[93] Journal Officiel. *Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique*, 5 Janvier 1988. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000875419.

[94] Marie Jung. Les sites web des agences régionales de santé (ars) piratés. *01net*, 09 Janvier 2014. http://pro.01net.com/editorial/611152/les-sites-web-des-agences-regionales-de-sante-ars-pirates/.

[95] Marie Jung. Les établissements de santé, proies faciles des pirates. *01Net*, 10 Janvier 2014. http://pro.01net.com/editorial/611694/les-etablissements-de-sante-proies-faciles-des-pirates/.

[96] Kaspersky. *KASPERSKY SECURITY BULLETIN 2013*, 3 Décembre 2013. http://media.kaspersky.com/pdf/KSB_2013_EN.pdf.

[97] kdawson. Why are cc numbers still so easy to find ? *Slashdot*, 24 May 2007. http://it.slashdot.org/story/07/05/24/136207/why-are-cc-numbers-still-so-easy-to-find.

[98] Sophos Labs. The conflict of autorun.inf. Blog officiel de Sophos, 16 Janvier 2009. http://nakedsecurity.sophos.com/2009/01/16/the-conflict-of-autoruninf/.

[99] Alexandre Laurent. Ddos sans précédent contre spamhaus : Internet va bien, merci pour lui. *Clubic Pro*, 28 Mars 2013. http://pro.clubic.com/it-business/securite-et-donnees/actualite-550362-spamhaus-ddos-cyberbunker.html.

[100] Damien Leloup. L'open-source n'est pas un modèle économique, c'est un modèle de développement. *Le Monde*, 30 Septembre 2010. http://www.lemonde.fr/technologies/article/2010/09/30/l-open-source-n-est-pas-un-modele-economique-c-est-un-modele-de-developpement_1417853_651865.html.

[101] Natasha Lomas. Europe's new cybercrime center to open its doors this week : Ec3 to act as hub for eu-wide collaboration to combat e-crime. *Tech Crunch*, 9 janvier 2013. http://techcrunch.com/2013/01/09/europes-new-cybercrime-center-to-open-its-doors-this-week-ec3-to-act-as-hub-for-eu-w

[102] JULIEN LÉCUYER. Le site internet de la mairie de saint-andré piraté par des islamistes. *La Voix du nord*, 14 Juillet 2014. http://www.lavoixdunord.fr/region/le-site-internet-de-la-mairie-de-saint-andre-pirate-par-ia22b129506n2272379.

[103] Marc-Etienne Léveillé. Os x/flashback - le premier logiciel malveillant à infecter des centaines de milliers d'ordinateurs mac. *Misc*, Septembre 2012. http://connect.ed-diamond.com/MISC/MISC-063/OS-X-Flashback-Le-premier-logiciel-malveillant-a-infecter-des-centaines-de-milliers-

[104] Jean-Marc Manach. Confidentiel — ne pas diffuser sur internet. *Bug Brother*, 20 aout 2014. http://bugbrother.blog.lemonde.fr/2014/08/20/confidentiel-ne-pas-diffuser-sur-internet/.

[105] Boris Manenti. Notre pire cauchemar, c'est le cyber-sabotage. *Obsession*, 21 janvier 2014. http://obsession.nouvelobs.com/hacker-ouvert/20140121.OBS3200/notre-pire-cauchemar-c-est-le-cyber-sabotage.html.

[106] Nathan Mattise. After blue screen of death reports, microsoft says to uninstall recent patch. *Ars Technica*, 17 aout 2014. http://arstechnica.com/information-technology/2014/08/after-blue-screen-of-death-reports-microsoft-says-to-uninstall-recent-patch/.

[107] Mc Afee. *Net Losses : Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II*, Juin 2014. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

[108] Hassan Meddah. http ://www.usinenouvelle.com/article/recruter-ses-experts-en-cybersecurite.n253722. *Usine Nouvelle*, 10 Avril 2014. http://www.usinenouvelle.com/article/recruter-ses-experts-en-cybersecurite.N253722.

[109] Ministère du Redressement Productif. *Nouvelle France industrielle : 34 plans de reconquête*. http://www.redressement-productif.gouv.fr/nouvelle-france-industrielle.

[110] Philippe Montarges. L'open source, un nouveau modèle économique pour la france ? *Les Echos*, 11 Septembre

2013. http://www.lesechos.fr/idees-debats/cercle/cercle-79553-lopen-source-un-nouveau-modele-economique-pour-la-france-1018942.php.

[111] Atif Mushtaq. Zero-day season is not over yet. Blog Officiel FireEye, 26 aout 2012. http://www.fireeye.com/blog/technical/cyber-exploits/2012/08/zero-day-season-is-not-over-yet.html.

[112] M. McDONOGH. *Cyberattaques dans l'UE*. Comité économique et social européen, 10 juillet 2014. http://eescopinions.eesc.europa.eu/viewdoc.aspx?doc=ces/ten/ten550/fr/EESC-2014-01488-00-00-AC-TRA-fr.doc.

[113] NetCraft. April 2014 web server survey. Blog Officiel, Avril 2014. http://news.netcraft.com/archives/2014/04/02/april-2014-web-server-survey.html.

[114] Nick Nguyen. Please read : Security issue on amo. Blog Officiel Mozilla Add-ons, Février 2010. http://blog.mozilla.org/addons/2010/02/04/please-read-security-issue-on-amo/.

[115] Moheeb Abu Rajab Fabia n Monro Niels Provos, Panayiotis Mavrommatis. All your iframe s point to us. *Google Technical Report*, 2008. http://static.googleusercontent.com/media/research.google.com/fr//archive/provos-2008a.pdf.

[116] Norton by Symantec. *2012 Norton Cybercrime Report*, 5 septembre 2012. http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf.

[117] Audrey Oeillet. La plus grande attaque ddos à ce jour vient de toucher l'europe et les etats-unis. *Clubic*, 12 Février 2014. http://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/cybercriminalite/actualite-618512-grande-attaque-ddos-toucher-europe-etats-unis.html.

[118] U.S. Department of Health & Human Services. Breaches affecting 500 or more individuals. http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

[119] OKTEY. Panorama des technologies antispam. Page Web. http://www.altospam.com/fr/panorama-des-technologies-antispam.php.

[120] Bernard Orr. Saudi aramco says virus shuts down its computer network. *Reuters*, 15 aout 2012. http://www.reuters.com/article/2012/08/15/us-aramco-virus-idUSBRE87E18S20120815.

[121] OSEO. *PME et Brevets, Regards sur les PME numéro 18*, 2009. http://www.bpifrance-lelab.fr/content/download/1532/12950/version/1/file/Regards_PME_18_Brevet.pdf.

[122] Yves ; Osterwalder, Alexander ; Pigneur and Christopher L. Tucci. Clarifying business models : Origins, present, and future of the concept. *Communications of the Association for Information Systems : Vol. 16, Article 1*, 2005. http://aisel.aisnet.org/cais/vol16/iss1/1.

[123] Timothy Grance Peter Mell. *The NIST Definition of Cloud Computing, Special Publication 800-145*. NIST, Septembre 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[124] Guillaume Pierre. Cloud et sécurité : le point sur 7 questions qui fâchent. *Les Echos*, 9 Avril 2013. http://business.lesechos.fr/directions-numeriques/cloud-et-securite-le-point-sur-7-questions-qui-fachent-6004.php.

[125] Guillaume Pierre. Protéger les données sensibles des entreprises. *Les Echos*, 9 Avril 2013. http://business.lesechos.fr/directions-numeriques/proteger-les-donnees-sensibles-des-entreprises-5950.php.

[126] Ponemon Institute. *Managing Cyber Security as a business Risk : Cyber Insurance in the Digital Age*, Aout 2013. http://assets.fiercemarkets.com/public/newsletter/fiercehealthit/experian-ponemonreport.pdf.

[127] Ponemon Institute. *2014 Cost of Data Breach Study : Global Analysis*, Mai 2014. http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/.

[128] Ponemon Institute. *The Risk of an Uncertain Security Strategy Study of Global IT Practitioners in SMB Organizations*, Novembre 2013. http://sophos.files.wordpress.com/2013/11/2013-ponemon-institute-midmarket-trends-sophos.pdf.

[129] Marie-Cécile Renault. Les patrons de pme sont gagnés par le ≪ras-le-bol fiscal≫. *Le Figaro*, 22 Novembre 2011. http://www.lefigaro.fr/conjoncture/2013/11/22/20002-20131122ARTFIG00527-les-patrons-de-pme-sont-gagnes-par-le-ras-le-bol-fiscal.php.

[130] Jerome Saiz. Faille rtf : elle infecte aussi à la preview d'un email. Blog Qualys, 4 avril 2014. http://magazine.qualys.fr/menaces-alertes/faille-rtf-word-outlook-preview/.

[131] Craig Schmugar. Signed malware : You can run, but you can't hide. Blog Officiel McAfee, 23 mars 2012. http://blogs.mcafee.com/mcafee-labs/signed-malware-you-can-runbut-you-cant-hide.

[132] Sophos. Operation aurora hack was counterespionage, not china picking on tibetan activists. Blog Officiel Sophos, 22 mai 2013. http://www.vupen.com/english/.

[133] Bernhard Plattner Brian Trammel Stefan Frei, Dominik Schatzmann. Modelling the security ecosystem - the dynamics of (in)security. In Ross Anderson, editor, *Workshop on the Economics of Information Security (WEIS)*, Cambridge, UK, June 2009. http://www.techzoom.net/security-ecosystem.

[134] Kevin Stevens and Don Jackson. *ZeuS Banking Trojan Report*. Dell Secure Works, 11 Mars 2010. http://www.secureworks.com/cyber-threat-intelligence/threats/zeus/?threat=zeus.

[135] Christophe Devine Stéfan Le Berre. Peut-on faire confiance aux antivirus ? *Misc*, Janvier 2010. http://connect.ed-diamond.com/MISC/MISC-047/Peut-on-faire-confiance-aux-antivirus.

[136] Symantec. *February 2011 Intelligence Report*, 2012. http://www.messagelabs.com/mlireport/MLI_2011_02_February_FINAL-en.PDF.

[137] Symantec. *2014 Internet Security Threat Report, Volume 19*, Avril 2014. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

[138] Khaley (Symantec). A decade in review : Cybercriminal motivations behind malware. Blog de Symantec, 08 Septembre 2011. http://www.symantec.com/connect/blogs/decade-review-cybercriminal-motivations-behind-malware.

[139] Laurent Thévenin. Le bel avenir du marché de la cyber-assurance. *Les Echos*, 04 Février 2014. http://www.lesechos.fr/04/02/2014/LesEchos/21619-141-ECH_le-bel-avenir-du-marche-de-la-cyber-assurance.htm.

[140] Tred Micro. *The Business of Cybercrime, A Complex Business Mode*, Janvier 2010. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_business-of-cybercrime.pdf.

[141] Verizon. *2014 Data Breach Investigation Report (DBIR)*, 2014. http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf.

[142] Zack Whittaker. Microsoft admits patriot act can access eu-based cloud data. *ZDNet*, 28 Juin 2011. http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225.

[143] Wikipedia. Heartbleed. Page Web. http://fr.wikipedia.org/wiki/Heartbleed.

[144] Wikipedia. Loi des grands nombres. Page Web. http://fr.wikipedia.org/wiki/Loi_des_grands_nombres.

[145] Wikipedia. Révélation d'edward snowden. Page Web. http://fr.wikipedia.org/wiki/R%C3%A9v%C3%A9lations_d%27Edward_Snowden.

[146] Wikipedia. Stuxnet. Page Wikipedia. http://fr.wikipedia.org/wiki/Stuxnet.

[147] Wikipédia. Clé usb u3. Site Web. http://fr.wikipedia.org/wiki/Cl%C3%A9_USB_U3.

[148] Soren Seelow Yves Eudes. Le logiciel espion blackshades au coeur d'une grande enquête internationale. *Le Monde*, 23 Mai 2014. http://www.lemonde.fr/societe/article/2014/05/23/le-logiciel-espion-blackshades-au-coeur-d-une-grande-enquete-internationale_4424783_3224.html.

[149] Zithom. Pedophilie et malware. Blog, 2009. http://zythom.blogspot.fr/2009/11/pedophilie-et-malware.html.

[150] John Zorabedian. How malware works : Anatomy of a drive-by download web attack (infographic). Blog Officiel Sophos, 26 Mars 2014. http://blogs.sophos.com/2014/03/26/how-malware-works-anatomy-of-a-drive-by-download-web-attack-infographic/.